STUDY

Requested by the LIBE committee

European Parliament

Strengthening Europol's mandate

A legal assessment of the Commission's proposal to amend the Europol Regulation

Policy Department for Citizens' Rights and Constitutional Affairs
Directorate-General for Internal Policies
PE 694.200 - May 2021

EN

Strengthening Europol's mandate

A legal assessment of the Commission's proposal to amend the Europol Regulation

Abstract

This study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee, aims to provide background information on the current legal framework of Europol and a legal assessment of the European Commission's proposal of 9 December 2020 to strengthen Europol's mandate, divided in thematic blocks. The legal assessment is accompanied by policy recommendations.

This document was requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs.

AUTHORS
Dr Niovi VAVOULA, Lecturer in Migration and Security, Queen Mary University of London
Prof. Valsamis MITSILEGAS, Professor of European Criminal Law and Global Security, Queen Mary University of London

ADMINISTRATOR RESPONSIBLE
Alessandro DAVOLI

EDITORIAL ASSISTANT
Christina KATSARA

LINGUISTIC VERSIONS
Original: EN

ABOUT THE EDITOR
Policy departments provide in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact the Policy Department or to subscribe for updates, please write to:
Policy Department for Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
Email: poldep-citizens@europarl.europa.eu

Manuscript completed in May 2021

This document is available on the internet at:
http://www.europarl.europa.eu/supporting-analyses

CONTENTS

LIST OF ABBREVIATIONS

ACER	European Agency for the Cooperation of Energy Regulators
AFSJ	Area of Freedom, Security and Justice
AI	Artificial Intelligence
AWF	Analysis Work File
CEPOL	European Union Agency for Law Enforcement Training
CJEU	Court of Justice of the European Union
COSI	Standing Committee on Operational Cooperation on Internal Security
DPA	Data Protection Authority
DPO	Data Protection Officer
EBCGA/FRONTEX	European Border and Coast Guard Agency
EC3	European Cybercrime Centre
ECHR	European Convention on Human Rights
EDPS	European Data Protection Supervisor
EFECC	European Financial and Economic Crime Centre
EIS	European Information System
EMPACT	European Multidisciplinary Platform Against Criminal Threats
EMSC	European Migrant Smuggling Centre
ENISA	European Union Agency for Cybersecurity
ENLETS	European Network of Law Enforcement Technology Services
ENU	Europol National Unit
EPPO	European Public Prosecutor's Office
EUIPO	European Union Intellectual Property Office

Eu-LISA	European Union Agency for the Operational Management of Large-Scale IT Systems
Eurojust	European Union Agency for the Criminal Justice Cooperation
Europol	European Union Agency for Law Enforcement Cooperation
EU	European Union
FIU	Financial Information Unit
FRA	European Union Agency for Fundamental Rights
IOCTA	Internet Organised Crime Threat Assessment
IRU	Internet Referral Unit
JHA	Justice and Home Affairs
JIT	Joint Investigation Team
JPSG	Joint Parliamentary Scrutiny Group
LIBE	Committee on Civil Liberties, Justice and Home Affairs
MASP	Multi-Annual Strategic Plans
NGO	Non-Governmental Organisation
OAPs	Operational Action Plans
OLAF	European Anti-Fraud Office
OSP	Online Service Provider
PNR	Passenger Name Record
QUEST	Querying Europol's systems
SIENA	Secure Information Exchange Network Application
SIRENE	Supplementary Information Request at the National Entries
SIS	Schengen Information System
SOCTA	Serious and Organised Crime Threat Assessment

TEU	Treaty on the European Union
TFEU	Treaty on the Functioning of the European Union
UNODC	United Nations Office on Drugs and Crime
US	United States

EXECUTIVE SUMMARY

Background

In the field of police cooperation, the European Union Agency for Law Enforcement Cooperation (Europol), the legal basis of which is Regulation (EU) 2016/794 (Europol Regulation), has a key role in supporting cooperation among the EU Member States in the area of cross-border law enforcement. On 9 December 2020, the Commission presented a proposal for a Regulation amending the Europol Regulation, aiming at enhancing Europol's mandate. The proposal encompasses a wide-ranging revision of Europol's tasks, which can be divided in nine themes as follows:

(**1) Enabling Europol to cooperate effectively with private parties;**

(2) Enabling Europol to process large and complex datasets;

(3) Strengthening Europol's role on research and innovation;

(4) Enabling Europol to enter data into the Schengen Information System (SIS);

(5) Strengthening Europol's cooperation with third countries;

(6) Strengthening Europol's cooperation with the European Public Prosecutor's Office (EPPO);

(7) Enabling Europol to request the initiation of an investigation of a crime affecting a common interest covered by an EU policy;

(8) Strengthening the data protection framework applicable to Europol; and

(9) Other provisions, including enhancing political accountability and parliamentary scrutiny.

Aim

This study aims to provide the European Parliament with background information on Europol's legal framework, a legal analysis of the proposal to revise the Europol Regulation and policy recommendations so that the study can contribute to the preparation of a forthcoming legislative report of the LIBE Committee on the revision of Europol's mandate.

Key findings

From the outset, the study stresses that the **proposal entails widespread reforms to Europol's mandate**, **which transform the nature of the agency and its relationship with the Member States**. The reforms have been proposed even though the Europol Regulation **has not been subject to an evaluation yet**. Scarce information is included in the Impact Assessment accompanying the proposal and some EU documentation, which cannot replace the lack of a proper evaluation. As a result, the effectiveness and impact of the agency cannot be fully and properly assessed.

(**1) Enabling Europol to cooperate effectively with private parties**: This reform concerns the enhancement of cooperation between Europol and private parties in countering criminal offences committed in abuse of the cross-border services of private parties. The proposal aims to establish the agency as a central point of contact in cases of multi-jurisdictional or non-attributable datasets. Europol will be enabled to: (a) receive personal data directly from private parties on a more regular basis; (b) inform such private parties of missing information; and (c) ask Member States to request private parties to share further information. Additionally, Europol can provide its infrastructure for the exchange of data between national authorities and private parties and support Member States in preventing large scale dissemination of terrorist content or violent extremism.

The study finds that these changes constitute a considerable paradigm shift for the agency, which is line with **the emergence of the trend in past years to establish direct channels of communication between law enforcement and private parties and foster a public/private partnership. Applying this approach to the case of Europol requires detailed rules on the duties of Europol, Member States and the private sector, e.g. when the private parties may refuse to cooperate, as well as provisions on independent authorisation of transfers and remedies for individuals**. The study points out that the concept of 'private parties' is open-ended and there are no limitations as to the nature of private parties. Whereas certain safeguards are included, e.g. the requirement for 'absolute' or 'strict' necessity, there are additional safeguards that are mentioned in the Impact Assessment, but not explicitly stated in the proposal. It is further argued that the **European Data Protection Supervisor (EDPS) could be involved before the agency makes such transfers**. In addition, whereas the proposal **proscribes systematic, massive or structural transfers** in cases where the private party is outside the EU, this is not extended to those private parties within the EU. Finally, it must be ensured that Europol's role in supporting Member States to prevent the dissemination of online content related to terrorism and violent extremism conforms with the Europol's role as foreseen in the recently approved Regulation on preventing the dissemination of terrorist content online.

(2) Enabling Europol to process large and complex datasets: This reform aims to address the so-called 'big data challenge' following the admonishment of the agency by the EDPS on 17 September 2020. The proposal aims to enable Europol to conduct 'pre-analyses' of large and complex datasets received and identify whether these concern individuals whose personal data may be processed by Europol in line with Annex II of the Europol Regulation. Another proposed provision aims to enable the pre-analysis in support of a criminal investigation following transmission of an investigative case file to Europol. The study notes that **it is welcome that the prior processing is limited to a maximum period of one year, which can be extended following authorisation by the EDPS.** One suggestion is to define the terms 'large datasets' and 'digital forensics' and explicitly delimit processing when there is **an objective necessity**, so as to ensure that the derogation of Article 18(5a) does not become the rule. Clear criteria to determine that it is justified to extend the maximum period of pre-analysis must be laid down and it could be useful to consider that **prior to each pre-analysis the EDPS must be at least informed and that the DPO must provide authorisation**. The relationship between the new rules and the existing derogation under Article 18(6) must also be clarified, as well as the relationship between the two new provisions foreseen. As these rules constitute an exception, their application must be strict and the existence of a link to an on-going investigation is crucial. In addition, the Regulation should lay down certain conditions and/or thresholds, such as scale, complexity, type or importance of investigations. Finally, the involvement of the EDPS not only in cases where an investigative case file is submitted by a third country, but in general in supervising the processing of large and complex datasets should be maintained and enhanced.

(3) Strengthening Europol's role on research and innovation: Europol will process personal data for research and innovation matters for the development of tools, including the use of AI for law enforcement. When developing new technologies **extensive processing of large quantities of personal data** may be required, for example to create and test algorithms or for encryption. Therefore, the potential impact of such processing for research and innovation purposes to the principle of non-discrimination and the rights to respect for private life and protection of personal data must be guaranteed. The processing of personal data for research and innovation should take place **only if needed in order to reach the objectives of the project**. Furthermore, the processing of **synthetic, anonymised or pseudo-anonymised personal data, as opposed to real operational data must be preferred, where possible**, **and the processing of special categories of personal data must be explicitly excluded or accompanied by additional safeguards. Moreover, principles of data**

protection law—in particular the principles of data minimisation, data quality and privacy by design and by default—must be taken into account.

(4) Enabling Europol to enter data into the Schengen Information System (SIS): Currently, Europol has 'read-only' access to all types of alerts stored in SIS. The proposal creates a new alert category that Europol can use to enter alerts into SIS following consultation with the Member States and after authorisation by the Executive Director. A detailed process for the issuance of so-called 'information alerts' is foreseen in a separate proposal amending Regulation (EU) 2018/1862 (COM(2020) 791 final). This study doubts whether this power, which to an extent equates Europol with Member States, fits within Europol's mandate, as laid down in Article 88 TFEU. It is also questionable whether Europol will be able to conduct a proper quality check before issuing alerts in SIS. Importantly, the study questions the operational value of such alerts, as they provide significant discretion to national authorities to follow up and wide divergences may arise in practice. The impact on individuals whose personal data will be inserted in SIS is significant and potential liability issues may also arise if the quality of data contained in the alert is not high. The possibility to delimit these alerts to those concerning terrorism has been proposed as an alternative, but this study is concerned that this is only an intermediate step before further expanding Europol's powers to enter alerts in the system.

(5) Strengthening Europol's cooperation with third countries: The proposal foresees a (seemingly minor) change enabling the Executive Director to authorise not only transfers, but also categories of transfers of personal data to third countries or international organisations in specific situations and on a case-by-case basis. The study finds that it is not clear what exactly is meant by 'categories of transfers' and this reform may broaden the remit of such transfers from criminal investigations on specific suspects to surveillance activities in general, thus changing Europol's powers. However, the study also notes that Member States wish to further expand Europol's capabilities to exchange personal data with third countries by transplanting the wording of Directive (EU) 2016/680 (Law Enforcement Directive) and Regulation (EU) 2018/1727 (Eurojust Regulation) to the Europol legal framework, and thus creating a new legal ground for exchanges of personal data on the basis of appropriate safeguards outside the three already prescribed grounds. The study finds that this reform poses significant legal challenges as it bypasses existing institutional safeguards and undermines the importance of an adequacy decision **and the procedure for assessing the data protection framework of a third country as adequate**, in violation of the constitutional limits placed by the Court of Justice of the EU (CJEU) in *Schrems*.

(6) Strengthening Europol's cooperation with the European Public Prosecutor's Office (EPPO): This reform concerns the reinforcement of Europol's cooperation with the EPPO in the aftermath of the adoption of Regulation (EU) 2017/1939 (EPPO Regulation) on the establishment of the EPPO. The study considers that the proposal is not fully aligned with the rules of the EPPO Regulation and minor modifications to the text are necessary.

(7) Enabling Europol to request the initiation of an investigation of a crime affecting a common interest covered by an EU policy: The proposal aims to enable Europol to request competent authorities of a Member State to initiate, conduct or coordinate an investigation of a crime which affects a common interest covered by an EU policy regardless of the cross-border nature of the crime. However, the necessity of this reform has not been substantiated and effectively removes control from judicial authorities over the opening of their investigations in cases affecting one Member State only.

(8) Strengthening the data protection framework applicable to Europol: The proposal enhances Europol's data protection framework by extending the reach of Article 3 and Chapter IX of Regulation (EU) 2018/1725 to the work of Europol and explicitly adding biometric data within special categories of personal data. The study welcomes this reform, but considers that further alignment is necessary, particularly by entrusting the EDPS with the general powers laid down in Article 58 of Regulation (EU) 2018/1725.

(9) Other provisions, including enhancing political accountability and parliamentary scrutiny: In addition to the other reforms further expanding and clarifying Europol's tasks, the proposal aims to enhance political accountability and parliamentary scrutiny by enabling the Joint Parliamentary Scrutiny Group (JPSG) to receive information regarding the matters falling under themes (1)-(4), as discussed above. However, the study points out that, despite the establishment of the JPSG and the proposed amendments, parliamentary scrutiny and oversight remain weak. Shortcomings concern the structure and work of the JPSG, including the weak powers of the Group in the participation to and appointment of Europol's Management Board. With the addition of new tasks to Europol, the need to ensure a better framework for parliamentary oversight and political scrutiny must be emphasised.

1. INTRODUCTION

1.1. Background information

In recent years, European integration in criminal matters has been advanced through the setting up and operation of a number of EU bodies and agencies with responsibilities within the sphere of criminal law.[1] In the field of police cooperation in particular, the work of the European Union Agency for Law Enforcement Cooperation (Europol) is central in supporting cooperation among the EU Member States in the area of cross-border law enforcement. Europol's legal basis Regulation (EU) 2016/794 (Europol Regulation), adopted under the ordinary legislative procedure following the entry into force of the Lisbon Treaty, has been applicable since 1 May 2017.[2] Europol is described as the EU's 'criminal information hub'[3] and the main 'information broker',[4] as it facilitates information exchange between EU Member States, Europol, other EU bodies, international organisations and third countries, and produces criminal intelligence on the basis of information acquired from various sources, including Member States and its partners. Amongst its many tasks, Europol also supports and coordinates cooperation on cross-border police work and produces regular assessments that offer comprehensive, forward-looking analyses of crime and terrorism in the EU.

Overall, Europol is one of the key agencies in the development of an Area of Freedom, Security and Justice (AFSJ) and an important cog in the internal security architecture. In the Commission Communication on the Security Union Strategy of 24 July 2020, Europol features prominently in the shaping of the strategy and it is stressed that it 'faces a number of serious constraints […] which hinders it from effectively supporting Member States in combating terrorism and crime'.[5] Furthermore, in the Declaration of the Home Affairs Ministers on 'Ten points on the future of Europol' of 21 October 2020,[6] Europol's added value was praised and a series of issues were identified for further improvement so that the agency can become the first point of contact for combating crime in the EU (both within the EU and externally), a service provider for Member States with strong, active input on matters of content and organisation from the Member States and a place of innovation in forensics, artificial intelligence and big data analysis. Those recommendations broadly correspond to Europol's own comments on its experience with the implementation of the Europol Regulation, emphasising on its ability to process information, particularly large and complex datasets, and its cooperation with external partners.[7]

---

[1] The authors wish to thank Andreas Karapatakis, Ph.D. Candidate at Queen Mary University of London for his research assistance in the development of the study.

[2] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA [2016] OJ L135/53 (Europol Regulation).

[3] 'Europol Strategy 2020+' (*Europol,* 5 February 2019) <https://www.europol.europa.eu/publications-documents/europol-strategy-2020> accessed 3 May 2021, 4.

[4] Thomas Wahl, 'The European Union as an Actor in the Fight Against Terrorism' in Marianne Wade and Almir Maljevic (eds), A War on Terror? (Springer 2010) 144.

[5] Commission, 'Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee and the Committee of the Regions on the EU Security Union Strategy' COM(2020) 605 final, 21.

[6] Council, 'Declaration of the Home Affairs Ministers of the European Union - Ten points on the future of Europol' (21 October 2020).

[7] Europol, 'Europol's main operational considerations in light of the Europol Regulation' (14 July 2020), which may be found here <https://www.statewatch.org/media/1284/eu-europol-operational-considerations-legal-basis-edoc-1119771v3.pdf> accessed 3 May 2021.

In light of the above, on 9 December 2020, the Commission presented a proposal for a Regulation amending the Europol Regulation, aiming at enhancing Europol's mandate and strengthening its tasks to address emerging threats, including those posed by the Covid-19 pandemic.[8] Alongside the proposal, the Commission also released (on the same day) a Communication on a Counter-Terrorism Agenda for the EU,[9] signalling that Europol's reform has been influenced by the reinforced counter-terrorism efforts in the aftermath of terrorist events in the EU in 2020.[10] Scratching below the surface, the proposal encompasses a wide-ranging revision of Europol's tasks, which the Council has divided in nine thematic blocks.[11]

The themes are the following:

Thematic block 1: **enabling Europol to cooperate effectively with private parties**;

Thematic block 2: **enabling Europol to process large and complex datasets**;

Thematic block 3: **strengthening Europol's role on research and innovation**;

Thematic block 4: **enabling Europol to enter data into the Schengen Information System (SIS)**;

Thematic block 5: **Strengthening Europol's cooperation with third countries**;

Thematic block 6: **Strengthening Europol's cooperation with the European Public Prosecutor's Office (EPPO)**;

Thematic block 7: **Enabling Europol to request the initiation of an investigation of a crime affecting a common interest covered by an EU policy**;

Thematic block 8: **Strengthening the data protection framework applicable to Europol**; and

Thematic block 9: **Other provisions, including enhancing political accountability and parliamentary scrutiny**.

Following the adoption of the proposal, in its Conclusions on internal security and European police partnership of 14 December 2020,[12] the Council emphasised the key role of Europol, as one of the cornerstones of the European security architecture[13] in supporting Member States and their competent authorities in operations and investigations and in promoting cooperation[14] and underlined the *future* direction of Europol, as laid down in the Declaration.[15]

On 17 December 2020, the European Parliament adopted a resolution on the EU Security Union Strategy for the period 2020-2025. In paragraph 26, the Parliament 'takes note of the Commission's plan to revise Europol's mandate to enable it to become a hub for the exchange of information on law

[8] Commission, 'Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU0 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation' COM(2020) 796 final (Europol proposal of 2020).

[9] Commission, 'Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee and the Committee of the Regions - A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond' COM(2020) 695 final.

[10] Commission, 'Europol proposal of 2020' (n 8) 1.

[11] See Council, Document 5397/21 (19 January 2021). See 'EU: More powers for Europol: what does your government think?' (*Statewatch*, 15 March 2021) <https://www.statewatch.org/news/2021/march/eu-more-powers-for-europol-what-does-your-government-think/> accessed 3 May 2021.

[12] Council, Document 13083/1/20 (24 November 2020).

[13] ibid 5.

[14] ibid 20.

[15] ibid 5.

enforcement and for cooperation in the fight against terrorism and serious and organised crime in the EU'.

1.2. Objective of the study

Against this backdrop, the **aim of this study** is to provide the European Parliament with **background information** on Europol's current legal framework and **a legal analysis of the Commission proposal to revise the Europol Regulation** by exploring how Europol could deliver better operational support, expertise and criminal intelligence to Member States' law enforcement authorities in line with its mandate and fundamental rights, as enshrined in the EU Charter of Fundamental Rights (Charter), particularly the rights to respect for private life (Article 7) and the right to the protection of personal data (Article 8). The study also offers **policy recommendations to contribute** to the preparation of a forthcoming **legislative report** of the LIBE Committee on the **revision of the Europol mandate**, following the adoption of the Commission's proposal.

1.3. Methodology

This study is based on desk research and the review of existing available reports, studies and analyses from sources and documents primarily from EU institutions, agencies and bodies, as well as academia and civil society. It principally encompasses legal instruments and policy documents of EU institutions, bodies and agencies, such as Council documents examining aspects of the proposal, resolutions of the European Parliament or Europol documentations. An analysis of EU primary and secondary legislation from the perspective of fundamental rights, as interpreted in the jurisprudence of the Court of Justice of the European Union (CJEU), is central to this research. With regard to the possibility of enabling Europol to record alerts in SIS, the study also provides an assessment of the legislative proposal that was adopted to amend the SIS legal framework[16] so as to provide a holistic approach to that issue. In view of the ongoing examination of the proposals within the Council, the analysis is updated until 3 May 2021.

1.4. Structure

This study is structured as follows: Section 2 provides a concise sketch of the current legal framework of Europol, so as to inform the subsequent analysis. Section 3 is devoted to the analysis of the content of the proposal amending Europol's mandate. In order to provide a holistic approach to the proposed amendments, the analysis is divided into specific themes, which correspond to the thematic blocks that are currently examined by the Council. Within each theme, the current legal framework is set out, including its possible shortcomings, and all relevant amendments envisaged in the proposal are examined in the light of the protection of fundamental rights. The last sub-section of Section 3 is dedicated to issues relating to the need to ensure a better framework to provide parliamentary oversight and political scrutiny, thus enhancing Europol's democratic legitimacy. These issues are thus discussed separately from thematic block 9, in more detail, providing suggestions outside the legislative proposal. Finally, Section 4 provides an overall assessment of the proposal, as well as policy recommendations.

[16] Commission, 'Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters as regards the entry of alerts by Europol' COM(2020) 791 final (SIS proposal).

2. THE EUROPOL LEGAL FRAMEWORK

Headquartered in The Hague since 1999, Europol is tasked with supporting and strengthening cooperation between EU Member States in the area of cross-border police cooperation. Its identity and mission have developed over the years through a series of legislative reforms. The first legal basis, the Europol Convention,[17] which was signed in 1995 and entered into force in 1998, was supplemented by a series of legal acts—mostly Protocols—which clarified and extended Europol's mandate and tasks.[18] In 2009, the Europol Convention was replaced by the Europol Council Decision,[19] and with a view to *inter alia* enhancing Europol's role in information exchange, governance and accountability. In the post-Lisbon era, Europol's legal framework was replaced by the Europol Regulation legally based on Article 88 of the Treaty on the Functioning of the European Union (TFEU). The Regulation is applicable to all EU Member States since 1 May 2017, except Denmark,[20] which has an opt-out in the area of justice and home affairs, in accordance with Protocol 22 to the Lisbon Treaty, but still cooperates with Europol on the basis of a specific agreement.[21]

This section provides a concise overview of Europol's legal framework, focusing on the provisions of the Europol Regulation, with the aim to inform the subsequent analysis. A more detailed examination of those provisions under reform is provided in the next Section.

2.1. Organisation and structure

The main organs of Europol are the (intergovernmental) Management Board, composed of one representative per Member State and one representative of the Commission (each having one vote) and taking most of its decisions by a majority of its members,[22] and the Executive Director.[23] The Management Board is responsible for a wide range of matters concerning the functioning of Europol, such as the adoption of the working programmes,[24] and it proposes to the Council a shortlist of candidates for the posts of Executive Director and Deputy Executive Directors,[25] who are eventually appointed by the Council.[26] The Executive Director is Europol's legal representative, manages Europol and is responsible for the day-to-day administration.[27]

Europol has a two-fold relationship with Member States: through the Europol National Units (ENUs), and through the liaison officers seconded at Europol. On the one hand, the national unit is the 'liaison

[17] Council Act of 26 July 1995 drawing up the Convention Based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention) [1995] OJ C316/1.

[18] For an analysis see Valsamis Mitsilegas and Fabio Giuffrida, 'Bodies, Offices and Agencies' in Valsamis Mitsilegas, *EU Criminal Law* (2nd edn, Hart forthcoming 2021).

[19] Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol) [2009] OJ L121/37 (Europol Council Decision). For an overview see among others Alexandra De Moor and Gert Vermeulen, 'The Europol Council Decision: Transforming Europol into an Agency of the European Union' (2010) 47(4) Common Market Law Review 1089; Emma Disley and others, 'Evaluation of the implementation of the Europol Council Decision and of Europol's activities' (Technical Report for Europol Management Board, Rand Europe, 2012).

[20] Europol Regulation, recital 74.

[21] See Council Implementing Decision (EU) 2017/290 of 17 February 2017 amending Decision 2009/935/JHA as regards the list of third States and organisations with which Europol shall conclude agreements [2017] OJ L42/17.

[22] Europol Regulation, art 15(1). Under the Europol Convention, most of the decisions of the Management Board had to be taken by unanimity, whereas Article 37(8) of the Europol Council Decision lowered the quorum to two thirds.

[23] Europol Regulation, arts 9 and 10(1).

[24] Europol Regulation, art 11. The most sensitive decisions, such as the working programmes and the budget, are adopted with a majority of two-thirds of the members of the Board.

[25] Europol Regulation, art 11(1)(j).

[26] Europol Regulation, arts 54 and 55.

[27] Europol Regulation, art 16(4) and (1) respectively. The Director's responsibilities are listed in art 16(5).

body' between Europol and domestic competent authorities,[28] though Member States *may* allow direct contacts 'subject to conditions determined by the Member States, including prior involvement of the national unit'.[29] One of the main tasks of ENUs is to supply Europol with the information necessary for the agency to fulfil its objectives.[30] However, in practice the effectiveness of this form of cooperation has been called into question, as police authorities are reported to be often reluctant to share their data with Europol.[31] This is arguably the problem of police cooperation *par excellence* in the EU, and national authorities are often urged to share their information with EU agencies on a more regular basis.[32] It is worth noting that the Regulation also tasks ENUs with raising 'awareness of Europol's activities,'[33] with the aim of increasing the knowledge about Europol among national authorities and, thus (potentially) the amount of information shared by them with the agency.[34] On the other hand, each national unit must send at least one Europol Liaison Officer to The Hague[35] to represent the interests of the national units within Europol.[36] Liaison officers have the task of assisting in the exchange of information between their Member States and Europol, as well as between their Member States and the liaison officers of other Member States, third countries and international organisations.[37]

2.2. Objectives and mandate

Article 3(1) of the Regulation provides that

> 'Europol shall support and strengthen action by the competent authorities of the Member States and their mutual cooperation in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy, as listed in Annex I'.[38]

Furthermore, Article 3(2) extends Europol's remit to related criminal offences, such as offences committed in order to facilitate or perpetrate––or procure the means of perpetrating––acts in respect of which Europol is competent, as well as to ensure the impunity of persons committing those same acts. Although the definitions of some forms of crime listed in Annex I have been harmonised at the European level, there are still variations from country to country. This may constitute an obstacle for the effective functioning of Europol, as 'the mandate of Europol is interpreted in different ways throughout the EU'.[39] Whereas practitioners seem to appreciate 'vague definitions that provide

[28] Europol Regulation, art 7(2).

[29] Europol Regulation, art 7(5).

[30] Europol Regulation, art 7(6)(a).

[31] See Maria Fletcher, Robin Lööf and Bill Gilmore, *EU Criminal Law and Justice* (Edward Elgar Publishing 2008) 91; Martijn Groenleer, *The Autonomy of the European Union Agencies: A Comparative Study of Institutional Development* (Uitgeverij Eburon 2009) 296; De Moor and Vermeulen (n 19) 1099; Disley and others (n 19) 47–65; Madalina Busuioc, *European Agencies. Law and Practices of Accountability* (OUP 2013) 146–150; Sabine Gless, 'Europol' in Valsamis Mitsilegas, Maria Bergström and Theodore Konstadinides (eds), *Research Handbook on EU Criminal Law* (Edward Elgar 2016) 459; Celine Cocq and Francesca Galli, 'The Evolving Role of Europol in the Fight Against Serious Crime: Current Challenges and Future Prospects' in Saskia Hufnagel and Carole McCartney (eds), *Trust in International Police and Justice Cooperation* (Hart 2017).

[32] However, see Europol Regulation, art 7(7).

[33] Europol Regulation, art 7(6)(c).

[34] Disley and others (n 19) 55–56.

[35] Europol Regulation, art 8(1).

[36] Europol Regulation, art 8(2).

[37] Europol Regulation, art 8(3) and (4) respectively. See also Groenleer (n 31) 293–294. On informality in the work of Europol but also its relationship with other EU bodies, see Didier Bigo and others, *The Field of the EU Internal Security Agencies* (L'Harmatan/Centre d'études sur les conflits 2007) 29.

[38] De Moor and Vermeulen (n 19) 1097.

[39] ibid 1098.

different options,'[40] the lack of a clear definition could create some '*uncertainty* over [the] competence [of Europol] to be involved in investigations'.[41]

2.3. Tasks

In order to fulfil its mandate, Article 4 of the Regulation lays down Europol's tasks, which could be divided into three broad categories: (a) information-related tasks; (b) operational tasks; and (c) tasks related to training, knowledge and expertise.

2.3.1. Information-related tasks: Producing criminal intelligence

As an 'enormous data processing agency rather than a law enforcing police office',[42] a central task of Europol is to '**collect, store, process, analyse and exchange information, including criminal intelligence**'.[43] Such data may derive from—within specific limits—private parties and persons, including private parties established in third countries.[44] The agency facilitates information exchange among national authorities, and between them and other relevant actors, including Europol itself.[45] In doing so, Europol is responsible for the management of SIENA (Secure Information Exchange Network Application), an online platform that aims to facilitate the exchange of information among Member States, EU bodies, third countries and international organisations.[46] National authorities highly value the exchange of information through SIENA,[47] not least because they are also allowed to exchange data concerning offences falling *beyond* the mandate of Europol.[48] However, this latter flow of information escapes the application of the agency's regime on data protection.[49]

Importantly, Europol **prepares 'threat assessments, strategic and operational analyses and general situation reports'**.[50] Europol's operational analysis may help to discover relevant information to be used for the purpose of (ongoing) national investigations and prosecutions, such as the precise location of people, goods or companies. It can also lead to discovering and establishing links among existing cases, of which Member States––via the national units––should be notified without undue delay.[51]

At the heart of Europol's analysis is the operation of a computerised information system. The Regulation brought about an important change in that respect. The Europol Convention and the Europol Council Decision listed the different components of this system, namely the Europol Information System (EIS), the analysis work files (AWFs) and the index function,[52] each of which

[40] Saskia Hufnagel, 'Organized Crime' in Valsamis Mitsilegas, Maria Bergström and Theodore Konstadinides (eds), *Research Handbook on EU Criminal Law* (Edward Elgar Publishing 2016) 363.

[41] ibid. Emphasis added.

[42] Gless (n 31) 465.

[43] Europol Regulation, art 4(1)(a). Emphasis added.

[44] Europol Regulation, arts 26 and 27.

[45] See Europol Regulation, art 4(1)(e), (h),(j) and (k).

[46] Europol Regulation, recital 24. Disley and others (n 19) 78.

[47] Disley and others (n 19) 36.

[48] ibid 61.

[49] Elspeth Guild and others, 'Implementation of the EU Charter of Fundamental Rights and its Impact on EU Home Affairs Agencies - Frontex, Europol and the European Asylum Support Office' (Study for the Civil Liberties, Justice and Home Affairs (LIBE) Committee of the European Parliament, 2011, PE 453.196) 70.

[50] Europol Regulation, art 4(1)(f).

[51] Europol Regulation, art 4(1)(b).

[52] Europol Council Decision, arts 11–13 (EIS), arts 14 and 16 (AWFs), and art 15 (index function). See previously Europol Convention, art 6(1). See André Klip, *European Criminal Law: An Integrative Approach* (3rd edn, Intersentia 2016) 490–492.

operated under different rules and objectives. The Regulation has adopted a new, simplified 'privacy by design approach'[53] so as to allow Europol to link and make analyses of relevant data, reduce delays in identifying trends and patterns and reduce multiple storage of data.[54] Thus, a new *integrated data management* strategy has been introduced, whereby the rules for information processing related to the data, rather than the systems of databases used to store them.[55] This new data processing paradigm has provided a wider degree of flexibility and increased information-related powers to Europol. However, it has raised significant concerns as regards the transparency of personal data processing and the purpose limitation principle; the structure of databases that operate in silos is precisely aimed at safeguarding that principle by preventing the linkage of data and the building of comprehensive profiles about individuals.[56] By removing the restrictions of architectural infrastructure, the Regulation has paved the way for the creation of an overarching EU database of criminal data and criminal intelligence[57] without detailing how the purpose limitation principle will be safeguarded. Operational effectiveness remains the key goal so that linkages between data and behavioural patterns may be discerned.

As for the preparation of threat assessments, Europol has a key role in shaping EU and domestic criminal policies through the production of Threat Assessments to assess and anticipate future threats and the groups of populations from which they are likely to emanate.[58] The Regulation expressly refers to the preparation of threat assessments, together with strategic analyses and general situation reports, among the agency's tasks.[59] The most known threat assessments are the SOCTAs (Serious and Organised Crime Threat Assessments), which are published every four years, TE-SATs (Terrorism Situation and Trend Reports) and IOCTAs (Internet Organised Crime Threat Assessments). Despite the criticism received,[60] Europol's threat assessments, particular SOCTA, set in motion a four-step cyclical process at the European level, the 'Policy Cycle',[61] to tackle the most important criminal threats through cooperation between EU Member States and institutions, as well as third countries and organisations.[62]

The perceived lack of flexibility resulting from data stored in different databases is discussed in Disley and others (n 19) 80–84.

[53] Europol Regulation, art 33.

[54] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA' COM(2013) 173 final, 8.

[55] 'Europol Strategy 2016-2020' (*Europol,* 19 May 2016) <https://www.europol.europa.eu/publications-documents/europol-strategy-2016-2020> accessed 3 May 2021, 12.

[56] Fanny Coudert, 'The Europol Regulation and Purpose Limitation: From the 'Silo-Based Approach' to … What Exactly?' (2017) 3(3) European Data Protection Law Review 313.

[57] ibid.

[58] 'Europol Strategy 2016-2020' (n 55). These tasks are arguably outside a clear constitutional framework since the Treaties do not envisage such a strong policy-making role for the agency. See Madalina Busuioc and Deirdre Curtin, 'The EU Internal Security Strategy, the EU Policy Cycle and the Role of (AFSJ) Agencies. Promise, Perils and Pre-requisites' (Study for the Civil Liberties, Justice and Home Affairs (LIBE) Committee of the European Parliament, 2011, PE 453.185) 7. See also Amadine Scherrer, Julien Jeandesboz and Emmanuel-Pierre Guittet, 'Developing an EU Internal Security Strategy, Fighting Terrorism and Organised Crime' (Study for the Civil Liberties, Justice and Home Affairs (LIBE) Committee of the European Parliament, 2011, PE 462.423) 88.

[59] Europol Regulation, art 4(1)(f). See also art 4(3).

[60] For criticism see Petrus C Van Duyne and Tom Vander Beken, 'The Incantations of EU Organised Crime Policy' (2009) 51(2) Crime, Law and Social Change 261, 273; and Scherrer, Jeandesboz and Guittet (n 58) 21–23. James Sheptycki, Hager Ben Jaffel and Didier Bigo, 'International Organised Crime in the European Union' (Study for the Civil Liberties, Justice and Home Affairs (LIBE) Committee of the European Parliament, 2011, PE 462.420) 8.

[61] See Artur Gruszczak, 'The EU Criminal Intelligence Model' in Joanna Beata Banach-Gutierrez and Christopher Harding (eds), *EU Criminal Law and Policy - Values, Principles and Methods* (Routledge 2017).

[62] Council, 'Conclusions on the creation and implementation of a EU policy cycle for organised and serious international crime' (Council of the European Union, Justice and Home Affairs Council meeting, Brussels, 8 and 9 November 2010).

In particular, with the adoption of the SOCTA and the identification of priorities in the fight against serious international and organised crime, each of these priorities are translated into Multi-Annual Strategic Plans (MASP) defining the strategic goals to achieve and setting out the policy. The MASP are implemented by Operational Action Plans (OAPs) include joint actions by Member States and agencies, as well as agencies' actions and national actions. The joint actions are carried out as EMPACT (European Multidisciplinary Platform Against Criminal Threats) projects to coordinate actions by Member States and EU organisations against the identified threats. EMPACT is a structured multidisciplinary co-operation platform of the relevant Member States, EU institutions and agencies, as well as third countries, international organisations and other (public and private) partners to address the prioritised threats of organised and serious international crime.

2.3.2. Operational tasks

As regards **operational** tasks, Europol is empowered to request national authorities both to initiate a criminal investigation[63] and to set up a joint investigation team (JIT),[64] in which Europol may also participate. As regards the request for initiation of a criminal investigation, Member States are not obliged to comply with Europol's requests, but should at least give reasons for their refusal without undue delay, preferably within one month of receipt of the request.[65] However, they are not bound by this obligation when providing those reasons would jeopardise the success of an ongoing investigation or the safety of an individual, or would be contrary to the essential interests of the security of the state.[66] As regards the request to set up a JIT, Europol participates in JITs in so far as these teams investigate criminal offences falling within Europol's mandate.[67] In a broadly worded provision, Europol officials may assist in all activities and (informal) exchanges of information with all members of the JIT[68] and may provide the latter with the necessary information processed by Europol itself.[69] Under certain conditions laid down in the Regulation, information obtained by Europol officials may be subsequently processed by the agency, with the consent and under the responsibility of the Member State which provided the information.[70] Europol may also propose the setting up of a JIT and assist national authorities in the procedures thereof.[71] However, in accordance with Article 88(3) TFEU, there is a general and all-encompassing prohibition for the agency to apply coercive measures in carrying out its tasks,[72] including tasks performed within JITs.[73] Furthermore, Europol may '*coordinate, organise and implement investigative and operational actions* to support and strengthen actions by the *competent authorities* of the Member States'.[74]

[63] Europol Regulation, art 6.

[64] Europol Regulation, art 5.

[65] Europol Regulation, art 6(3).

[66] ibid.

[67] Europol Regulation, art 5(1).

[68] Conny Rijken, 'Joint Investigation Teams: Principles, Practice, and Problems. Lessons Learnt from the First Efforts to Establish a JIT' (2006) 2(2) Utrecht Law Review 99, 117.

[69] Europol Regulation, arts 5(2) and (3). See Bart de Buck, 'Joint Investigation Teams: The Participation of Europol Officials' 8(2) ERA Forum 253, 259; Groenleer (n 31) 280; Guild and others (n 49) 29.

[70] Europol Regulation, art 5(4).

[71] Europol Regulation, arts 4(1)(d) and 5(5).

[72] Europol Regulation, art 4(5).

[73] For criticism see Mitsilegas and Giuffrida (n 18).

[74] Europol Regulation, art 4(1)(c). See 'Europol Strategy 2016-2020' (n 55) 16.

2.3.3. Training, knowledge and expertise

Europol develops, shares and promotes knowledge of crime prevention methods, investigative procedures and technical and forensic methods, provides advice to Member States,[75] and engages in the specialised training of national authorities.[76] In addition, Europol has developed EU centres of specialised expertise to respond to the threats to the EU internal security posed by large-scale criminal and terrorist networks,[77] including the Central Office for combating euro counterfeiting,[78] the European Migrant Smuggling Centre (EMSC), the European Counter Terrorism Centre (ECTC), the EU Internet Referral Unit (IRU), the European Cybercrime Centre (EC3)[79] and the European Financial and Economic Crime Centre (EFECC).

2.4. Processing of personal data and data protection

As the EU criminal information hub, safeguarding the rights to respect for private life and the protection of personal data, as enshrined in Articles 7 and 8 of Charter and Article 16(1) TFEU, is crucial. Europol is subject to an autonomous data protection regime, which applies to its work as *lex specialis*. Overall, the Regulation distinguishes between processing of operational personal data (for the purpose of attaining the agency's objectives) and non-operational or administrative personal data[80]—Europol's data protection safeguards are applicable to the first group only. As for the second group, the general data protection rules under Regulation (EU) 2018/1725 on the processing of personal data by EU institutions, bodies, offices and agencies apply.[81]

Whereas the majority of the rules below are currently subject to reform and therefore are presented in more detail in the next Section, it is worth providing already at this stage a concise outline of the basic rules for information processing. Chapter IV of the Regulation prescribes basic rules for the processing of information by Europol concerning:

- The sources of information that Europol may process: information may come from Member States, EU bodies, third countries, international organisations, private parties and private persons, in accordance with the rules and procedures provided for in the Regulation;[82] however, Europol may also retrieve and process information––including personal data––both

[75] Europol Regulation, art 4(1)(g) (emphasis added).

[76] Europol Regulation, art 4(1)(i) (emphasis added).

[77] Europol Regulation, art 4(1)(l) (emphasis added). As for Europol's role vis-à-vis cybercrime, see also Europol Regulation, art 4(1)(m) and Recital 8.

[78] Europol Regulation, art 4(4). See Groenleer (n 31) 287.

[79] For cybercrime, see Ben Hayes and others, 'The Law Enforcement Challenges of Cybercrime: Are We Really Playing Catch-Up?' (Study for the Civil Liberties, Justice and Home Affairs (LIBE) Committee of the European Parliament, 2015, PE 536.471) 33–35; Gless (n 31) 472–473. On ECTC and EC3, see Sabine Gless and Thomas Wahl, 'A Comparison of the Evolution and Pace of Police and Judicial Cooperation in Criminal Matters: A Race Between Europol and Eurojust?' in Chloé Brière and Anne Weyembergh (eds), *The Needed Balances in EU Criminal Law: Past, Present and Future* (Hart Publishing 2018) 343.

[80] Europol Regulation, recital 53 and art 46.

[81] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC [2018] OJ L 295/39.

[82] Europol Regulation, art 17(1).

from publicly available sources[83] and, if allowed by specific legal instruments, from EU, international and national information systems.[84]

- The purposes of information processing activities: Europol may process information 'in so far as necessary for the achievement' of its objectives, namely (1) cross-checking aimed at identifying connections or relevant links between information related to suspected or convicted criminals—the wording used here replicates the categories of persons whose data could be inserted in EIS, as outlined above; (2) strategic or thematic analyses; (3) operational analyses; and (4) facilitating exchanges of information between Member States, Europol and other EU bodies, as well as third countries and international organisations.[85]
- The obligation for the entity that shares its information with Europol to determine the *purpose* for which that information is to be processed by the agency (purpose limitation).[86]
- The *access* to information stored by the agency: only *Member States* have the right to access and search all information provided to Europol for the purposes of *cross-checking* or *strategic analysis*.[87] Eurojust and OLAF, as well as Member States when information provided for operational analysis is concerned, can only have an *indirect access*, on the basis of a hit/no-hit system.[88]
- The obligation of Europol to notify a Member State, without delay, of any information concerning it.[89]

Further rules are contained in Chapter V of the Regulation on *inter alia* general data protection principles,[90] procedures for the assessment of reliability of the source and accuracy of information[91] and for the processing of special categories of personal data[92] –although biometric data are not listed as a special category,[93] time limits for the storage and deletion of data,[94] measures for the security of processing,[95] data protection by design,[96] right of access of individuals to their personal data and right to rectification, erasure and restriction,[97] obligation of prior consultation of the EDPS in specific cases,[98] and responsibility in data protection matters.[99]

---

[83] For some positive views on information that Europol can retrieve from publicly available sources see Daniel Drewer and Vesela Miladinova, 'The BIG DATA Challenge: Impact and Opportunity of Large Quantities of Information Under the Europol Regulation' (2017) 33(3) Computer Law & Security Review 298, 303–304.

[84] Europol Regulation, art 17(2) and (3) respectively. According to article 17(3), where data retrieved from EU, international or national legal instruments, those instruments will prescribe access and use of that information by Europol, in so far as they provide for stricter rules on access and use than those laid down by the Europol Regulation.

[85] Europol Regulation, art 18.

[86] Europol Regulation, art 19(1).

[87] Europol Regulation, art 20(1).

[88] Europol Regulation, arts 20(2) (Member States) and 21 (Eurojust and OLAF).

[89] Europol Regulation, art 22.

[90] Europol Regulation, art 28.

[91] Europol Regulation, art 29.

[92] Europol Regulation, art 30.

[93] See Florin Coman-Kund, 'Europol's International Exchanges of Data and Interoperability of AFSJ Databases' (2020) 26(1) European Public Law 181, 193.

[94] Europol Regulation, art 31.

[95] Europol Regulation, art 32.

[96] Europol Regulation, art 33.

[97] Europol Regulation, arts 36 and 37.

[98] Europol Regulation, art 39.

[99] Europol Regulation, art 38.

Supervision of Europol's data processing activities is entrusted to the Data Protection Officer (DPO) and the European Data Protection Supervisor (EDPS). The DPO is a member of Europol's staff who acts 'independently' in the performance of their duties to ensure the internal application of the Regulation to the activities of Europol concerning the processing of data,[100] and therefore has access to all the data processed by the agency and all its premises.[101] The EDPS monitors and ensures the application of the Regulation provisions related to the protection of individuals' rights concerned by the processing of personal data by Europol.[102] They advise individuals, as well as Europol, on matters concerning personal data.[103]

The fruits of this supervision are already visible; as it will be examined in detail in Section 3.3, on 17 September 2020, the EDPS found that the way operational analyses of Europol is conducted on the basis of large amounts of information (so-called big data) which is stored for several years is not supported by its legal framework and goes against the data minimisation principle.[104] Indeed, Article 18(3) of the Regulation requires the determination of *inter alia* the categories of personal data and the categories of data subjects, both of which are further circumscribed by Article 18(5). The EDPS admonished Europol, in a bold move that has sent shockwaves through the agency, the core work of which is based on the processing of large datasets.[105]

2.5. Exchanges of personal data with partners

In response to calls to enhance Europol's efficiency, the Regulation provides the legal framework for the agency to exchange data with a wide range of public and private authorities both within and outside the EU, in particular with EU bodies,[106] third countries and international organisations,[107] private parties,[108] and private persons.[109] The basic principles governing such exchanges of personal data could be summarised as follows:

- Information cannot be processed if it has 'clearly' been obtained in 'obvious' violation of human rights.[110]
- Europol may receive and process personal data from partners 'in so far as necessary and proportionate for the legitimate performance of its tasks'[111] and subject to the conditions provided for in Articles 23–27 of the Regulation.
- Europol may transfer personal data to its partners, if necessary for preventing and combating crimes for which Europol is competent and 'if the recipient gives an undertaking that the data will be processed only for the purpose for which they were transferred';[112] if the data have been provided by a Member State, the latter should also give its consent––which can be withdrawn

[100] For the list of the DPO's tasks, see Europol Regulation, art 41(6).
[101] Europol Regulation, art 41(8).
[102] Europol Regulation, art 43(1).
[103] ibid.
[104] EDPS, 'EDPS Decision of 17 September 2020 relating to EDPS own initiative inquiry on Europol's big data challenge' (2020).
[105] Council, Document 11512/20 (9 October 2020).
[106] Europol Regulation, art 24.
[107] Europol Regulation, art 25.
[108] Europol Regulation, art 26.
[109] Europol Regulation, art 27.
[110] Europol Regulation, art 23(9). This overarching principle is also enshrined in Recital 39 of Europol Regulation.
[111] Europol Regulation, art 23(5).
[112] Europol Regulation, art 23(6).

at any time––unless it 'has granted its prior authorisation to such onward transfer';[113] similarly, if a Europol partner intends to transfer data held by Europol, the agency should give its prior explicit authorisation.[114]

- Europol should *record* all transfers of personal data and the grounds for such transfers.[115]

Once these conditions are met, Europol can directly transfer personal data to another EU body.[116] Over the years, Europol has concluded a number of agreements with EU bodies, including the European Union Agency for the Criminal Justice Cooperation (Eurojust), the European Anti-Fraud Office (OLAF), the European Union Agency for Law Enforcement Training (CEPOL), the European Union Agency for Law Enforcement Training (EBCG/Frontex), the European Union Intellectual Property Office (EUIPO), the Commission, the European Central Bank and the EPPO.[117]

As for Europol's relations with third countries and international organisations, prior to the entry into force of the Lisbon Treaty, Europol had concluded sixteen 'operational' agreements and four 'strategic' agreements,[118] with third countries and some international organisations, namely the World Customs Organization and the United Nations Office on Drugs and Crime (UNODC), as well as with Interpol. In the aftermath of the Lisbon Treaty, however, the power to conclude international agreements rests only with the Council, in accordance with Article 218 TFEU. Therefore, Europol may exchange information, including personal data, with third countries and international organisations on the basis of the Council's agreements, which should adduce 'adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals'.[119] However, three further options are available. First, Europol may exchange information with international partners pursuant to previously signed operational agreements,[120] which remain valid.[121] Second, information with third countries or international organisations can also be exchanged if the Commission has adopted an 'adequacy decision'.[122] Finally, the Executive Director can authorise the transfer of personal data to third countries and international organisations on a case-by-case basis for certain exceptional––but arguably broadly worded––reasons.[123]

As regards private parties and private persons, Europol may exchange information, including personal data, with them in accordance with stringent conditions[124] provided for in Articles 26 and 27 of the Regulation. In particular, personal data from private persons and bodies may be processed as far as they are received via ENU or via a contact point or a competent authority of a third country which is subject to an adequacy decision of the Commission, or with which an (operational) agreement has been signed (either by Europol or by the Council).[125] Second, Europol should not contact private parties

[113] ibid.

[114] Europol Regulation, art 23(7).

[115] Europol Regulation, art 23(8).

[116] Europol Regulation, art 24.

[117] The text of these agreements, as well as a list of all Europol's partners may be found here: <https://www.europol.europa.eu/partners-agreements> accessed 3 May 2021.

[118] Europol's international dimension has been examined in-depth by Florin Coman-Kund, *European Union Agencies as Global Actors: A Legal Study of the European Aviation Safety Agency, Frontex and Europol* (Routledge 2018) 274-328.

[119] Europol Regulation, art 25(1)(b).

[120] Europol Regulation, art 25(1)(c).

[121] Europol Regulation, art 25(4).

[122] Europol Regulation, art 26(1)(a).

[123] See Europol Regulation, art 25(5).

[124] Europol Regulation, recital 23.

[125] Europol Regulation, arts 26(1) and 27(1).

and persons to retrieve information.[126] In exceptional circumstances, and on a case-by-case basis, Europol can transfer personal data only to private parties (even if established outside the Union) but not to private persons.[127]

2.6. Judicial control

Subjecting Europol to the judicial control of the CJEU has been a particularly contentious issue.[128] With the adoption of the Lisbon Treaty, the Court has now full jurisdiction as regards preliminary rulings concerning the AFSJ. Overall, the Europol Regulation has thus enhanced judicial control,[129] particularly when potential violations of the rules on data protection occur. First, Europol can be brought before the CJEU by an individual who has suffered damage as result of an unlawful data processing operation and who claims their right to receive compensation in accordance with Article 340 TFEU.[130] Second, pursuant to Article 48 of the Europol Regulation, the decision of the EDPS on a complaint lodged in accordance with the Europol Regulation is subject to the judicial review of the CJEU.[131] Finally, the EDPS can refer a matter to the CJEU under the conditions provided for in the TFEU.[132] However, most of the acts and decisions through which Europol accomplishes its mission still escape the scrutiny of the CJEU, such as the requests to initiate a criminal investigation or to set up a JIT, as well as all other acts adopted by Europol in its supporting and coordinating activities.[133]

2.7. Democratic accountability and parliamentary scrutiny

'Light' accountability is achieved primarily by adopting and submitting annual Europol activity reports to the European Parliament, the Council, the Commission, the Court of Auditors and the national parliaments.[134] Whereas prior to the adoption of the Europol Regulation oversight of the agency was fairly limited, democratic accountability has been enhanced through the establishment of a specialised Joint Parliament Scrutiny Group (JPSG).[135] The latter was established in April 2017 with the task to scrutinise Europol's activities in fulfilling its mission[136] 'including as regards the impact of those activities on the fundamental rights and freedoms of natural persons'.[137] To that end, the JPSG is *inter alia* consulted by the Management Board on the multi-annual programming of Europol[138] and is recipient of a number of documents concerning its activities, such as threat assessments and other strategic analyses and reports, as well as the annual reports drafted by the Management Board. Though this reform has been praised as having the potential to enhance the transparency of a sector which 'has

[126] Europol Regulation, arts 26(9) and 27(4).

[127] Compare art 26(5) and (6) with art 27(5) of the European Regulation.

[128] See Malcolm Anderson et al*, Policing the European Union* (Clarendon Press 1995) 207-209; John D Occhipinti, *The Politics of EU Police Cooperation - Toward a European FBI?* (Lynne Rienner 2003) ch 3.

[129] Europol Regulation, art 49(2) and (4) respectively.

[130] Europol Regulation art 50(1).

[131] For instance, Europol's decisions denying or restricting the right of access to personal data can be appealed before the EDPS (Europol Regulation, art 36(7)).

[132] Europol Regulation, art 43(3)(h).

[133] Mitsilegas and Giuffrida (n 18).

[134] Europol Regulation, art 11(1)(c). As for the accountability of the Management Board see also Europol Regulation, art 50(2).

[135] See art 88(2) TFEU. Europol staff and EU officials supported the European Parliament's involvement in the activities of Europol––in so far as it does not concern the operational ones (see Disley and others (n 19) 141–143).

[136] See Gless and Wahl (n 79) 352–353.

[137] Europol Regulation, art 51(2).

[138] Europol Regulation, art 51(2)(c).

inherent characteristics of secrecy,'[139] its effectiveness has been called into question for numerous reasons, including the structure of the JPSG, which are explained in Section 3.11. In addition, two further forms of accountability are achieved via transparency, in particular access to documents, and via the administrative inquiries of the European Ombudsman to which Europol can be subject.[140]

2.8. Europol's effectiveness

Overall, Europol's contribution to the fight against cross-border crime is increasingly appreciated,[141] but ultimately Europol's effectiveness largely depends upon the willingness of national authorities to share information with the agency. Indeed, Europol's ability to bring about results is tightly related to Member States' 'input and participation'.[142] The more domestic authorities and bodies resort to Europol, the more the latter is in a condition to carry out its operational and strategic tasks and collect useful information in view of further sharing relevant knowledge. Somehow paradoxically, 'Europol cannot oblige Member States to cooperate and it relies entirely on Member States' willingness to participate'. At the same time, however, in its more than twenty-year history, Europol has often struggled with the reluctance of national authorities that were, and are, sometimes not very keen to share their data with the agency. This shows that the degree of trust between the Member States and Europol has still not reached a high level, which is confirmed by the Council Conclusions of 14 December 2021 that call on Member States to make full use of the existing instruments for sharing information, including Europol.[143] To some extent, this hesitance can be attributed to a scarce knowledge of Europol's work, to which the not always transparent and somewhat secret functioning of the agency may have contributed, especially at the beginning of its activities.

[139] Meijers Committee, 'Note on the interparliamentary scrutiny of Europol' (CM 1702) 3. See also Ian Cooper, 'A New Form of Democratic Oversight in the EU: The Joint Parliamentary Scrutiny Group for Europol' (2018) 10(3) Perspectives on Federalism 185.

[140] Europol Regulation, art 69.

[141] See Saskia Hufnagel, *Policing Global Regions: The Legal Context of Transnational Law Enforcement Cooperation* (Routledge 2021).

[142] See also Groenleer (n 31) 298.

[143] Council, Document 13083/1/20 (n 12) para 19.

3. THE REFORM OF THE EUROPOL REGULATION

3.1. Widespread reforms without prior evaluation

As outlined in the introduction, the proposal to reform Europol's mandate contains a series of widespread reforms that **fundamentally change the powers of the agency and the relationship it has with Member States and other partners**. This is particularly the case of public/private partnerships (Section 3.2), the relationship with SIS (Section 3.5) and requests for the initiation of investigations beyond cross-border cases (Section 3.8), which raise questions as to whether Europol's mandate can support these changes. Whereas each theme will be examined in detail on its own, it is important to stress this major paradigm shift already here, because although the proposal is accompanied by a two-part Impact Assessment,[144] **it is not based on an evaluation in line with the Better Regulation Guidelines.**[145] The need for prior evaluation was prescribed by Article 68 of the Europol Regulation, which reads:

> 'By 1 May 2022 […] the Commission shall ensure that an evaluation assessing, in particular, the impact, effectiveness and efficiency of Europol and of its working practices is carried out. The evaluation may, in particular, address the possible need to modify the structure, operation, field of action and tasks of Europol'.

In light of the above, the timing of the proposal raises concerns *vis-à-vis* the ability to fully evaluate the effectiveness and performance of Europol's work, due to the limited and scattered information on how the agency currently operates. Some information is contained in the Impact Assessment,[146] which, however, cannot in any way replace an evaluation of the Europol Regulation. In the introduction, it was also stated that Europol provided its own comments in preparation for the proposal,[147] but this patchwork approach is neither complete not satisfactory. The impact and efficiency of Europol and its working practices, as well as any shortcomings in Europol's mandate, ought to have been identified through a full evaluation prior to the adoption of the proposal, particularly since the reforms are so extensive.

3.2. Enhancing cooperation with third parties

This thematic block concerns the enhancement of cooperation between Europol and private parties in countering criminal offences committed in abuse of the cross-border services of private parties, such as internet-based, financial services or telecommunications providers. Illustrative examples in that respect involve sex offenders who abuse children and share pictures and videos worldwide using web platforms, terrorists who use the internet to recruit new volunteers and cyber criminals who use phishing and social engineering to commit scams, ransomware attacks and payment fraud.[148]

---

[144] Commission, 'Staff Working Document – Impact Assessment Report accompanying the document Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/79, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation Part 1/2' SWD(2020) 543 final (Europol Impact Assessment Part 1); Commission, 'Staff Working Document – Impact Assessment Report accompanying the document Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/79, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation Part 2/2' SWD(2020) 543 final (Europol Impact Assessment Part 2'.

[145] 'Better Regulation Guidelines' <https://ec.europa.eu/info/sites/default/files/better-regulation-guidelines-better-regulation-commission.pdf> accessed 3 May 2021.

[146] Commission, 'Europol Impact Assessment Part 2' (n 144) 38-45.

[147] Europol, 'Europol's main operational considerations' (n 7).

[148] Commission, 'Europol Impact Assessment Part 1' (n 144) 17.

3.2.1. Existing cooperation between Europol and third parties

Private parties hold increasing amounts of personal data relevant for criminal investigations; therefore, as the Council conclusions of December 2019 on Europol's cooperation with private parties stated, they 'play a growing role in preventing and countering cyberenabled crimes' and there is need for 'legal certainty if they are to transfer personal data to Europol'.[149] This is all the more necessary in cases of datasets that are non-attributable, which means that the relevant jurisdiction is unclear, or multi-jurisdictional, whereby the datasets contain information relevant to many jurisdictions. Amending the rules on the cooperation between Europol and private parties also features in the Declaration of the Home Affairs Ministers on 'Ten points on the future of Europol', which was agreed on 21 October 2020, whereby it is stated that 'Europol must therefore be enabled to cooperate effectively with private parties, in accordance with the needs of the Member States and respecting their national legislation'.[150]

Member States may not have the necessary resources or they may miss the whole intelligence picture if, for example, they receive limited datasets from private parties related to their jurisdiction. Furthermore, Europol is allowed to exchange personal data with private parties, but Article 26 of the Europol Regulation provides a series of restrictions; as outlined in Section 2.5, **the traditional way for the agency to receive personal data from private parties is indirectly via competent intermediaries** (national units, contact points of third countries or international organisations with which Europol can exchange personal data or an authority of a third country or an international organisation which is the subject of an adequacy decision).[151] As indicated in the Impact Assessment accompanying the Commission proposal, the assessment of that personal data by Europol is done 'in a technically isolated way without analysing it against other data in its systems, without enriching this data with further analysis and within a specific four-month timeframe'.[152] According to the Council Conclusions of 2 December 2019 this can cause 'considerable delays and ultimately render such data obsolete or no longer relevant for investigation or analysis.[153] In another Council Document, it is stated that the current mandate of Europol is also insufficient on certain occasions, for example when cooperation with private parties on personal data may be required repeatedly in joint operations specifically on the cybercrime aspects.[154]

Moreover, **where private parties proactively exchange personal data directly with Europol, the latter may process that data only to identify the responsible ENU**, transfer the dataset to it and then delete it.[155] ENUs may resubmit the data to Europol.

In addition, as a general rule, **Europol is prohibited from transferring personal data directly to private parties, with three exceptions**: if (a) the transfer is undoubtedly in the interests of the data subject; (b) the transfer is absolutely necessary in the interests of preventing the imminent perpetration of a crime; or (c) if the transfer concerns publicly available data and is strictly necessary for preventing and combating internet-facilitated crimes (the so-called system of referrals).

3.2.2. Exchanges of personal data with private parties under scrutiny

Exchanges of personal data between Europol and private parties have been subject to a study conducted by Milieu and published in November 2020, as mandated by Article 26(10) of the Europol

[149] Council, Document 14745/19 (2 December 2019).

[150] Council, 'Declaration of the Home Affairs Ministers' (n 6) pt 8.

[151] Europol Regulation, art 26(1).

[152] Commission, 'Europol Impact Assessment Part 1' (n 144) 43.

[153] Council, Document 14745/19 (n 149).

[154] Council, Document 10494/20 (4 July 2019) which can be found here <https://www.statewatch.org/media/documents/news/2019/aug/eu-council-europol-private-parties-10494-19.pdf> accessed 3 May 2021.

[155] Europol Regulation, art 26(2)-(4).

Regulation;[156] that is the sole study evaluating aspects of the Regulation. The study was primarily based on responses received to a stakeholder consultation and semi-structured interviews followed by an online workshop.

With regard to indirect exchanges of personal data between Europol and private parties, the study found that Europol receives only a minority of the personal data that private parties transfer to the national law enforcement authorities, even though this data relates or could relate to a crime within Europol's mandate. On the one hand, national law enforcement authorities may not always transfer personal data to ENUs for various reasons, for example because the file must clearly suggest that the crime in question is within Europol's mandate or because the national authorities lose clear visibility of the steps taken by ENUs.[157] Importantly, ENUs are not always sharing data they received from private parties with Europol to a sufficient degree, but it is acknowledged that there might be legal reasons for not doing so.[158] In relation to direct exchanges, the study found that the system of referrals operates well and the system of Europol receiving personal data from private parties via an intermediary, typically national law enforcement authorities, is commonly used.[159] As for private parties sharing personal data directly with Europol outside the context of referrals, the study found shortcomings, as proactive sharing is rarely used, because it is perceived to be a complex, complicated and slow process.[160] Consequently, the study recommended the revision of the Europol Regulation to enable direct exchanges of personal data between Europol and private parties, and to empower Europol with a more extensive data processing mandate. As for national law enforcement authorities sharing personal data with private parties via Europol, the study found that national law enforcement authorities often require access to personal data held by private parties during their investigations, but might face obstacles (requests being refused, not answered or responses are incomplete or delayed) when trying to obtain personal data from private parties, mainly in connection with cross-border cases.[161]

However, as it has been rightly stressed,[162] the study suffers from numerous shortcomings: it did not discuss (the need for) independent judicial control and it does not properly reflect the views of national data protection authorities (DPAs) and private parties. Importantly, the relevance of the study to the negotiations of the E-evidence package, according to which law enforcement bodies will acquire access to electronic evidence in criminal matters, was not considered.[163] Finally, issues related to conflicts of law, jurisdiction and potential liabilities of online service providers were not examined in depth.

3.2.3. Direct exchanges of personal data with private parties and exchanges of personal data in crisis situations

In order to enhance Europol's role as a criminal information hub, the proposal extends the legal possibilities for exchanges of personal data with private parties, with **the agency essentially becoming a central point of contact in cases of multi-jurisdictional or non-attributable datasets. Europol will be enabled to: a) receive personal data directly from private parties on a more**

[156] Milieu, 'Study on the Practice of Direct Exchanges of Personal Data between Europol and Private Parties' (September 2020).

[157] ibid 44.

[158] ibid 44-45.

[159] ibid 29-35.

[160] ibid.

[161] ibid.

[162] Wouter van Ballegooij, 'Revision of the Europol Regulation' (January 2021) 5.

[163] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters' COM(2018) 225 final; 'Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings' COM(2018) 226 final.

regular basis; b) inform such private parties of missing information; and c) ask Member States to request private parties to share further information.

In particular, Article 4(1)(m) of the Europol Regulation concerning Europol's tasks in supporting Member States as regards internet-related offences is amended to add that the agency is enabled to coordinate law enforcement authorities' responses to cyber attacks and the taking down of terrorist content online.[164] Furthermore, a new task is added to empower Europol 'to support Member States' actions in preventing the dissemination of online content related to terrorism or violent extremism in crisis situations'.[165]

Furthermore, Article 26 is subject to considerable reforms.[166] Europol will be expressly allowed to receive data directly from private parties and process those personal data in order to identify all national units concerned.[167] Furthermore Article 26(4) is amended so that in cases where Europol receives personal data from a private party in a third country, then the result of the analysis and verification of such data is shared with the third country concerned. Moreover, as regards the possibility of transferring personal data to private parties, the proposal marks two shifts: first, the wording is somewhat different: **whereas under the current Regulation transfers are prohibited except if any of the three exceptions apply, as outlined above, the revised Article 26(5) has a permissive approach and enables transmissions or transfers in these three cases and adds a fourth one**: when the transmission or transfer of personal data is strictly necessary for Europol to inform that private party that the information received is insufficient to enable Europol to identify the national units concerned. In other words, **Europol is allowed to exchange personal data with private parties when it wishes to follow-up so as to notify the private party about information missing**. In such cases, certain conditions must be met: (i) the transmission or transfer follows a receipt of personal data directly from a private party; (ii) the missing information, which Europol may refer to in these notifications, has a clear link with the information previously shared by that private party; and (iii) the missing information must be strictly limited to what is necessary for Europol to identify the national units concerned.[168] In addition, Article 26(6), which regulates transfers of personal data to private parties outside the EU, is also amended to expressly include the transfers by Europol to follow-up on missing information. It is also clarified that such transfers are authorised by the Executive Director, and these should not take place if they determine that fundamental rights and freedoms of the data subject concerned override the public interest in the transfer. Finally, transfers must not be systematic, massive or structural.[169]

Europol is further **enabled to proactively reach out to private parties with a request for personal data**. In that respect, two additional provisions are inserted in Article 26. First, Europol may request Member States, via their ENUs, to obtain personal data from private parties, which are established or have a legal representative in their territory, under their applicable laws, for the purpose of sharing it with Europol. As a safeguard, the requested personal data must be strictly limited to what is necessary for Europol with a view to identifying the national units concerned. Furthermore, Member States shall ensure that their competent national authorities can lawfully process such requests in accordance with their national laws for the purpose of supplying Europol with the information necessary for it to fulfil its objectives.[170] Second, as indicated in proposed Article 26(6b), Europol's infrastructure may be used for exchanges between the competent authorities of Member States and private parties. In cases where

[164] Commission, 'Europol proposal of 2020' (n 8) art 1(2)(a)(iii).

[165] ibid art 1(2)(a)(iv). See new art 4(1)(u).

[166] ibid art 1(5)(a)(i). See art 18(2)(d).

[167] ibid art 1(12)(a). See art 26(2).

[168] ibid art 1(12)(c).

[169] ibid art 1(12)(c).

[170] ibid art 1(12)(d). See new art 26(6a).

Member States use this infrastructure for exchanges of personal data on crimes falling outside the scope of Europol's objectives, the agency shall not have access to that data.[171]

Another addition is the support of Europol to Member States in preventing the large-scale dissemination, via online platforms, of terrorist content related to on-going or recent real-world events depicting harm to life or physical integrity, or calling for imminent harm to life or physical integrity. In that respect, new Article 26a prescribes that Europol will serve as a channel for the exchange of personal data with private parties, including hashes, IP addresses or URLs related to such content. Whereas the wording of the Article 26a resembles revised Article 26, there are some notable differences, for example the transfer of personal data to private parties outside the EU is subject to authorisation by the Executive Director but there are no specific requirements to be met.[172] Furthermore, Europol must ensure that detailed records of all transfers of personal data and the grounds of such transfers are recorded and communicated upon request to the EDPS.[173] Finally, if the personal data received or to be transferred affect the interests of a Member State, Europol shall immediately inform the national unit of the Member State concerned.[174]

3.2.4. A paradigm shift with significant fundamental rights implications and insufficient safeguards

The proposed reforms will promote direct exchanges of personal data between Europol and private parties on a regular basis, in a **considerable paradigm shift** from the existing powers of the agency. This reform essentially aims to circumvent Member States' authorities by creating Europol as a focal point for collecting such data and distributing them accordingly. In that way, the agency will acquire information about potential cases even *before* the national authorities and solidify its involvement as early as possible, irrespective of whether national authorities would send the data to Europol or not. Magnifying Europol's role towards the direction of proactivity somewhat sits at odds with Article 88(1) TFEU, according to which Europol has a supportive role and its tasks are heavily relied on Member States' willingness to cooperate and **a 'greedy' Europol thus emerges**.

This shift further reflects **the emergence of the trend in the past years to establish direct channels of communication between law enforcement and private parties and foster a public/private partnership.** The E-evidence legislative package constitutes a prime example in this context and therefore lessons could be drawn from the ongoing negotiations to inform the present debate. Co-opting the private sector in the law enforcement context entails significant risks for the protection of fundamental rights, in particular privacy and protection of personal data. Questions about the ability of private parties to undertake the role of law enforcement authorities in scrutinising fully and effectively the fundamental rights implications of transfer of personal data held by them for the purposes of law enforcement also emerge in the present case of Europol, as the latter will be enabled to forward requests on behalf of Member States and proactively request information. Private parties also do not enjoy equality with public authorities in terms of cooperation and the same will also apply in the case of Europol. Therefore, private parties may find themselves in a subordinate position, being 'cornered' by both Europol and potentially Member States and thus under significant pressure to hand over the personal data requested.[175] Important safeguards, in particular obtaining prior judicial

[171] ibid art 1(12)(d). See new art 26(6b).

[172] ibid art 1(13). See new art 26a(4).

[173] ibid art 1(13). See new art 26a(6).

[174] ibid art 1(13). See new art 26a(7).

[175] See Valsamis Mitsilegas, 'The Privatisation of Mutual Trust in Europe's Area of Criminal Justice: The Case of E-evidence' (2018) 25(3) Maastricht Journal of European and Comparative Law 263; Sabine Gless and Pauline Pfirter, 'Cross-Border Access and Exchange of Digital Evidence: Cloud Computing Challenges to Human Rights and the Rule of Law' in Valsamis Mitsilegas and Niovi Vavoula (eds), *Surveillance and Privacy in the Digital Age: European, Transatlantic and Global Perspectives* (Hart 2021); Katalin Ligeti and Gavin Robinson, 'Sword, Shield and Cloud: Toward a European System of Public-Private Orders for Electronic Evidence in Criminal Matters?' in Valsamis Mitsilegas and Niovi Vavoula (eds), *Surveillance and Privacy in the Digital Age: European, Transatlantic and Global Perspectives* (Hart 2021); Sergio Carrera, Marco Stefan and

authorisation and scrutiny of compliance with fundamental rights risk bypassing. Therefore, **applying this approach to the case of Europol requires detailed rules on the duties of both Europol and the private sector, as well as provisions on independent authorisation of transfers and remedies for individuals**.

It is true that the revised provisions will not allow the agency to directly query databases managed by private parties. This was a policy option discussed in the Impact Assessment and discarded as more intrusive than the one preferred,[176] which does not oblige private parties to accept direct access by Europol to their databases. Such powers would also not have been compatible with Article 88(3) TFEU, which limits Europol's mandate and proscribes the application of coercive measures by Europol.[177] Furthermore, that option would clearly bypass applicable criminal procedural laws and the legal requirement for judicial approval so as to provide information to private authorities.

The reference to private parties more generally seems to suggest that **there are no limitations as to the nature of those private parties**, which may include non-governmental organisations (NGOs), as well as financial institutions. This raises questions about the relationship of this rule with Directive 1153/2019 on the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences.[178] In particular, it may result in situations where data reach Europol before they reach the relevant Member States. Similarly, it is vital to ensure non-interference with the tasks of Financial Intelligence Units (FIUs); Recital 33 of the proposal is relevant in that respect, explaining that any cooperation between Europol and private parties should not duplicate or interfere with the activities of FIUs and should only concern information not provided to them. The inclusion of that Recital to the text of the Europol Regulation is useful and has been preferred by the Member States.[179] However, further refinement of the scope of the term 'private parties' and the possible inclusion of NGOs within that term require further debate.

With respect to revised Article 26(5) on the possibility of Europol transferring personal data to private parties, it is welcome that in order to counter-balance the new powers of Europol the proposal maintains the existing specific safeguards, such as the requirement for 'absolute' or 'strict' necessity, as stated in Article 26(5) of the Europol Regulation. However, the difference between the terms 'transmission' and 'transfer,' which is observed in Article 26(5) is unclear and if these are different types of processing they must be defined. Moreover, **the reversed, permissive wording is also questionable and it must be examined whether such change is appropriate and necessary**.[180]

Importantly, as regards the new legal ground, further safeguards could be added in line with the Impact Assessment, which states that Europol will gather information to establish the jurisdiction of the Member States concerned over a form of crime falling within the agency's mandate. Arguably, this condition could be inferred from the wording of revised Article 26(5)(d)(iii), but it is not explicitly stated that the only purpose of the follow-up is that identification of the Member States concerned. That would be in line with Europol's role to support Member States so that the agency is prevented from acquiring autonomous powers to process personal data. In addition, the text could be enriched to

Valsamis Mitsilegas, 'Cross-Border Data Access in Criminal Proceedings and the Future of Digital Justice' (Centre for European Policy Studies, 2020).

[176] Commission, 'Europol Impact Assessment Part 1' (n 144) 49-50.

[177] EDPS, 'Opinion 4/2021' (8 March 2021) para 17.

[178] Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA [2019] OJ L186/122, Also see Council, Document 5527/4/21 (5 March 2021) 52-53.

[179] Council, Document 5388/2/21 (5 March 2021) 1, 34-35.

[180] Council, Document 5527/4/21 (n 178) 60, 73.

explicitly state that the request for information must be as targeted as possible,[181] and that an obligation on behalf of the private party will be imposed to share additional information.[182] Another question is whether the private party should be allowed to transfer the data received from Europol to any other party—it is vital that this is not allowed, especially in relation to those private parties located outside the EU, where the level of data protection may not be adequate under EU law.[183]

It must be added that an additional safeguard may be found in Article 1(37) of the proposal, stating that information on the number of exchanges with private parties must be provided to the JPSG to enhance transparency.[184] However, the Council has moved this provision in Article 7, adding that such information will be on the basis of quantitative and qualitative criteria defined by the Management Board and that the report will be sent to the European Parliament, the Council, the Commission and national parliaments.[185] However, this may not be sufficient oversight, and a way forward could be to **involve the EDPS before the agency makes such transfers, by inserting a requirement for the EDPS to be informed and by potentially involving the Europol DPO in decisions to follow up with private parties**.

As regards revised Article 26(6) concerning transfers of personal data to private parties established in third countries, it is welcome that **the proposal proscribes systematic, massive or structural transfers**; however, as noted by the EPDS, that provision relates only to cases of international transfers to private parties established outside the EU, and therefore **that safeguard should apply also to transmissions to private parties within the EU**.[186]

Furthermore, with respect to the possibility of Europol proactively requesting personal data via the national units from private parties, it must be noted that **the roles of Europol and Member States are unclear**. **Whereas Recital 31 of the proposal refers to multi-jurisdictional and non-attributable datasets, Article 26 makes no such distinction**. Furthermore, although the proposal foresees the application of additional safeguards, the text could be more explicit to include safeguards mentioned in the Impact Assessment, namely that a reasoned request shall be sent which should be as targeted as possible and should refer to the least sensitive data that is strictly necessary for Europol to establish the jurisdiction of the Member State concerned.[187] Interestingly, the Impact Assessment states that the Member States of establishment will assess the request *in light of the European interest*,[188] to ensure that the request does not go beyond what national law enforcement authorities of that Member State could request without judicial authorisation in terms of the type of information concerned, as well as with regard to the procedural aspects of the request. This reference to the 'European interest' requires further clarification. Moreover, the fact that national requests would have to be subject to prior judicial authorisation[189] and the provision of an effective remedy could also be mentioned in the text, as stressed in the Impact Assessment.[190] In addition, **it is uncertain whether Member States and private parties are obliged or may refuse to cooperate in this respect. If so, then this must be explicitly**

[181] EDPS, 'EDPS Formal comments on the draft Commission Implementing Regulation laying down rules and conditions for the operation of the web service and data protection and security rules applicable to the web service pursuant to Article 13 of Regulation (EU) 2017/2226 and repealing Commission Implementing Decision C(2019)1230' (13 February 2019) 6.

[182] European Union Agency for Fundamental Rights (FRA), 'Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Regulation on preventing the dissemination of terrorist content online' (12 February 2019) 38.

[183] Council, Document 5527/4/21 (n 178) 153, 138.

[184] FRA (n 182) 5.

[185] Council, Document 5388/2/21 (n 179) 26.

[186] EDPS, 'Opinion 4/2021' (n 177) para 18.

[187] Commission, 'Europol Impact Assessment Part 1' (n 144) 47.

[188] ibid.

[189] FRA (n 182) 23.

[190] ibid 28.

provided.[191] Finally, there is uncertainty as to whether following a request Europol could receive the data directly from the private party (thus the information would belong to Europol, and the latter would not have to inform the Member State(s) concerned) or through the Member State only (thus qualifying the information as national information).[192]

With regard to the role and responsibilities of Europol when acting as service provider to national authorities by offering its infrastructure for exchanges of data between Member States and private parties, these are not sufficiently clear as well. The only guidance offered is in the Impact Assessment, whereby in a footnote it is stated that '[i] these cases Europol acts as data processor rather than as data controller'.[193] The Europol Regulation does not define the notion of 'data processor'.[194] That said, the proposal also envisages that some provisions of Regulation (EU) 2018/1725 will be applicable to Europol, such as Article 3 and Chapter IX, as examined in Section 3.9, which will entail that Europol will have to comply with the conditions and obligations of a data processor in accordance with Article 87 of that Regulation. In view of the principle of accountability, there are a number of mandatory elements which should be provided for in a binding legal act under the EU or national law. Furthermore, in line with the recommendations of the EDPS, Europol should conduct an assessment of the possible security risks posed from the opening of its infrastructure for use by private parties and, where necessary, implement appropriate preventive and mitigating measures.[195]

The last aspect that merits attention concerns the addition of Article 26a regarding Europol's role in supporting Member States to prevent the dissemination of online content related to terrorism and violent extremism. It is recalled that Europol is already involved in removal of terrorist content online via the operation of EU Internet Referral Unit since July 2015, which is part of the EC3, with a mandate to refer terrorist and violent extremist content to Online Service Providers (OSPs) and support Member States and third parties in internet investigations. Furthermore, on 29 April 2021, the Regulation on preventing the dissemination of terrorist content online was adopted[196] and therefore the role of Europol should be aligned with the prescriptions of the new Regulation. These new provisions explicitly refer to Europol's tasks in issuing referrals, that is alerts hosting service providers of information for removal of terrorist content online, which are not affected.[197] Recital 36 also indicates that Europol will provide support to Member States in implementing the provisions of the forthcoming Regulation. Furthermore, Member States are encouraged to make use of the dedicated tools developed by Europol, such as the current Internet Referral Management application, which channels referrals on terrorist-related content and content to OSPs.[198] Hosting service providers should promptly inform the relevant authorities in the Member State concerned or the competent authorities of the Member State where they are established or have a legal representative of terrorist content involving an imminent threat to life or a suspected terrorist offence. In the case of doubt, hosting service providers should submit the information to Europol, which should provide the relevant follow-up action.[199] In addition, the competent authorities are encouraged to send copies of the removal orders to Europol to allow it to provide an annual report that includes an analysis of the

[191] See Council, Document 5527/4/21 (n 178) 61 -where the Commission answers to the affirmative- and 69, 70, 99. See Council, Document 5388/2/21 (n 179) 15, where Recital 31 reflects such change.

[192] Council, Document 5527/4/21 (n 178) 109.

[193] Commission, 'Europol Impact Assessment Part 1' (n 144) 13.

[194] EDPS, 'Opinion 4/2021' (n 177) para 19.

[195] ibid, para 20.

[196] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online [2021] OJ L 172/79**.**

[197] ibid recital 40.

[198] ibid recital 39.

[199] ibid art 14(5) and recital 41.

types of terrorist content subject to an order to remove it or to disable access thereto pursuant to this Regulation.[200]

Against this backdrop, in Article 26a of the proposal the authorisation of the Executive Director requires further criteria in line with those mentioned in Article 26(6). If this is not accepted, then a justification of the differentiated framework must be provided. Moreover, the definition of a 'crisis situation' is missing and its connection with other EU documents, such as the EU Crisis Protocol agreed in 2019 between the Commission, Member States and online service providers, must be specified.[201]

3.3. Addressing the 'big data challenge'

3.3.1. Europol's 'big data challenge' and the admonishment by the EDPS

This thematic block should be seen as the legislative response to the admonishment of Europol issued by the EDPS on 17 September 2020 regarding the so-called 'big data challenge'.[202] In a nutshell, as criminal investigations increasingly include the collection of large and complex datasets by national law enforcement authorities, over the past several years Member States have submitted such datasets to Europol for operational analysis with the aim of detecting links to other crimes and criminals in other Member States.[203] This practice brought to the fore concerns about the compliance of the processing of large datasets by Europol with the Europol Regulation, particularly its Articles 18(3) and 18(5). The latter limits the processing of personal data by Europol to the categories of data subjects listed in Annex II, namely suspects, convicted persons, persons regarding whom there are factual indications or reasonable grounds to believe that they will commit criminal offences, persons who might be called to testify in investigations or in subsequent criminal proceedings, victims, contacts and associates of a criminal and persons who can provide information on a crime. As the EDPS stressed, the provisions of Article 18 'apply and specify the principle of data minimisation for the processing of personal data for operational analysis purposes'.[204]

Such concerns were communicated by the Executive Director to the EDPS and in April 2019, the latter launched an inquiry on its own initiative on the use of Big Data Analytics by Europol for purposes of strategic and operational analysis. Overall, the EDPS found that large datasets—defined as datasets which, because of the volume, the nature or the format of the data they contain, cannot be processed with regular tools, but require the use of specific tools and/or storage facilities, [205] in particular digital forensics—do not allow from the outset to ascertain that all the information contained in these large datasets comply with the limitations prescribed in Article 18, with the volume of information so big that its content is often unknown until the moment when the analyst extracts relevant entities for their input into the relevant database.[206] These datasets are further stored even after the analysts have completed the extraction process in order to ensure that they can come back to the contribution in case of a new lead and to ensure the veracity, reliability and traceability of the criminal intelligence process.[207] As a result, the processing of large amounts of personal data does not comply with the Europol Regulation also because these are stored for several years, in violation of the principle of data minimisation, as defined by Article 28(1)(c) of the Europol Regulation. Importantly, there is a high

[200] ibid art 14(6).

[201] Commission, 'A Europe that Protects: EU Crisis Protocol: responding to terrorist content online' (October 2019) <https://ec.europa.eu/home-affairs/sites/default/files/what-we-do/policies/european-agenda-security/20191007_agenda-security-factsheet-eu-crisis-protocol_en.pdf> accessed 3 May 2021.

[202] See Section 2.4.

[203] Commission, 'Europol Impact Assessment Part 1' (n 144) 23-24.

[204] EDPS, 'EDPS Decision on the own initiative inquiry on Europol's big data challenge (5 October 2020) para 4.5.

[205] ibid para 1.

[206] ibid para 4.7.

[207] ibid para 4.8.

likelihood that Europol continually processes personal data on individuals for whom it is not allowed to do so and retain categories of personal data that go beyond Annex II.[208]

In light of the above, a structural legal issue has emerged due to the restrictions on personal data processing embedded in the Europol Regulation and the incompatibility with Europol's practices. The proposal thus aims to rectify this issue in line with the Declaration of the Home Affairs Ministers on 'Ten points on the Future of Europol', which underlined that Europol must be 'able to fulfil its tasks in the best possible way—at the same time, a high level of data protection must be guaranteed'.[209]

3.3.2. Enabling Europol to process large and complex datasets

In order to address this issue, the proposal provides a legal ground so that Europol can provide analytical support to the Member States by analysing large and complex datasets. To that end, Article 1(1)(c) of the proposal expands Europol's tasks in supporting Member States to identify persons whose involvement in crimes falling within the Europol's mandate constitute a high risk for security, and facilitate joined, coordinated and prioritised investigations. Furthermore, Article 1(5)(d) of the proposal introduces the possibility for Europol to carry out an initial processing—a 'pre-analysis' of personal data received pursuant to Article 17, for example by way of collation, prior to any further data processing, with the sole purpose of determining whether such data falls into the categories of data subjects as listed in Annex II.[210] This pre-analysis includes checking the data against all data that Europol already processes.[211] It is further proposed that the Management Board, acting on a proposal from the Executive Director and after consulting with the EDPS, will further specify the conditions relating to the processing of such data.[212] As an additional safeguard, Europol may only process personal data for a maximum period of one year, or in justified cases for a longer period with the prior authorisation of the EDPS, where necessary.[213] In addition, where the result of the processing indicates that personal data do not comply with the requirements of paragraph 5 of this Article, Europol shall delete that data and inform the provider of the data accordingly.[214]

Furthermore, according to new Article 18a, Europol may analyse such large and complex datasets, in support of a criminal investigation provided that two conditions are fulfilled: a) a Member State or the EPPO provides an investigative case file to Europol for the purpose of operational analysis in support of that specific criminal investigation within the mandate of Europol; and b) Europol assesses that it is not possible to carry out the operational analysis of the investigative case file without processing personal data outside the categories mentioned in Annex II. That assessment by Europol shall be recorded.[215] An 'investigative case file' is defined as 'a dataset or multiple datasets that a Member State, the EPPO or a third country acquired in the context of an on-going criminal investigation […] and submitted to Europol in support of that criminal investigation'.[216] Europol may process personal data contained in an investigative case file for as long as it supports the on-going specific criminal investigation for which the investigative case file was provided by a Member State or the EPPO, and only for the purpose of supporting that investigation.[217] The Management Board, acting on a proposal from the Executive Director and after consulting the EDPS, shall further specify the conditions relating

[208] ibid para 4.9.

[209] Council, 'Declaration of the Home Affairs Ministers' (n 6).

[210] Therefore, Article 18(5) is replaced to allow initial processing of personal data related to categories of individuals outside Annex II. See Commission, 'Europol proposal of 2020' (n 8) art 1(5)(c).

[211] ibid art 1(5)(d). See new art 18(5a).

[212] ibid.

[213] ibid.

[214] ibid art 1(5)(d). See new art 18(5a).

[215] ibid art 1(6). See new art 18a(1).

[216] ibid art 1(1)(c). See new art 2(q).

[217] ibid art 1(6). See new art 18a(2).

to the processing of such data.[218] Furthermore, personal data outside those listed in Annex II shall be functionally separated from other data and may only be accessed where necessary for the support of the specific criminal investigation for which they were provided.[219]

The investigative case file and the outcome of its operational analysis may be stored beyond the storage period, if requested by the Member State or the EPPO that provided an investigative case file to Europol, for the sole purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for as long as the judicial proceedings related to that criminal investigation are on-going in that Member State.[220] The same applies if judicial proceedings following a related criminal investigation are on-going in another Member State.[221] Also in this case, the Management Board, acting on a proposal from the Executive Director and after consulting the EDPS, shall further specify the conditions relating to the processing of such data.[222] And again, such personal data shall be functionally separated from other data and may only be accessed where necessary for the purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process.[223]

The aforementioned rules will also apply where Europol receives personal data from a third country with which there is an agreement concluded either with Europol or on the basis of Article 218 TFEU, or which is the subject of an adequacy decision, and such third country provides an investigative case file to Europol for operational analysis that supports the specific criminal investigation in a Member State or in Member States that Europol supports.[224] Where a third country provides an investigative case file to Europol, the EDPS shall be informed. Europol shall verify that the amount of personal data is not manifestly disproportionate in relation to the specific investigation in a Member State that Europol supports, and that there are no objective elements indicating that the case file has been obtained by the third country in manifest violation of fundamental rights. Where Europol, or the EDPS, reaches the conclusion that there are preliminary indications that such data is disproportionate or collected in violation of fundamental rights, Europol shall not process that data. Data processed pursuant to this paragraph may only be accessed by Europol where necessary for the support of the specific criminal investigation in a Member State or in Member States. It shall be shared only within the EU.[225]

3.3.3. Ensuring that an exception does not become the rule

The proposal addresses the legal gap through the introduction of a 'pre-analysis' of large and complex datasets received solely to separate necessary information, within the scope of Article 18(5) and Annex II, from data unrelated to criminal activity. The proposed approach is more restrictive than the alternative solution of introducing a new category of data subjects in Annex II of the Europol Regulation, which was examined in the Impact Assessment accompanying the proposal. That solution did not pass the necessity test, as it was (rightly) deemed more intrusive than the proposed option, which maintains the obligation on Europol to delimit its data processing activities to the specific categories of individuals laid down in Annex II.[226]

This reform will have substantial impact on the protection of personal data, as it will allow extensive data processing outside the remit of Annex II and beyond the current storage periods set out in the Europol Regulation. As such, it entails a significant limitation of the rights to respect for private life and protection of personal data. Therefore, sufficient safeguards must be introduced. Overall, **it is welcome**

[218] ibid.

[219] ibid.

[220] ibid art 1(6). See new art 18a(3).

[221] ibid.

[222] ibid.

[223] ibid.

[224] ibid art 1(6). See new art 18a(4).

[225] ibid art 1(6). See new art 18a(4).

[226] Commission, 'Europol Impact Assessment Part 1' (n 144) 51-52, 70-72.

that the prior processing is limited to a maximum period of one year, which can be extended following authorisation by the EDPS. Deletion of unnecessary data is also foreseen. As the EDPS has noted, these safeguards 'are generally in line with the data protection principles of purpose limitation and storage limitation'.[227] Another suggestion would be to enrich the Europol Regulation with **definitions of the term 'large datasets' and potentially that of 'digital forensics,'** which are the means used to analyse large and complex datasets.[228] These definitions are not found in the Europol Regulation or Regulation (EU) 2018/1725. Furthermore, in line with the Opinion of the EDPS, **this type of processing must be further limited to cases where the transfer by Member States to Europol and the subsequent processing of large datasets is actually an objective necessity**, so as to ensure that the derogation of Article 18(5a) does not become the rule.[229] This reference to strict necessity appears in the Impact Assessment[230] and in Recital 18 of the proposal, but it is not included in the text. Moreover**, it is unclear how the extension of the maximum period of pre-analysis will work in practice, given the lack of any indication and criteria to determine the existence of a 'justified case'**. Therefore, the EDPS has rightly pointed out that unless clear criteria are laid down there is a risk that the prior authorisation of the prolongation by the EDPS could actually turn into 'rubber stamping' of the requests of the agency.[231] Another potential safeguard to be added could be that **prior to each pre-analysis the EDPS must be at least informed and that the DPO must provide authorisation**.

In addition, **the relationship between the new derogation under 18(5a) and the existing derogation under Article 18(6) of the Europol Regulation, which enables processing of data for the purpose of determining whether such data are relevant to its task, requires clarification**.[232] Both provisions envisage 'temporarily processing of data' (pre-analyses) for similar, though not identical purposes and with different retention periods. Therefore, distinguishing between the application of Article 18(5a) and 18(6) is vital. In that respect, an evaluation of Europol would have been useful to provide specific indications as to when Europol has resorted to Article 18(6) and for which purposes. It must also be noted that Article 18(6) refers not only to 'conditions relating to the processing of such data', as Article 18(5a) states, but more specifically to 'conditions relating to the processing of such data, in particular with respect to access and use of the data, as well as time limits for the storage and deletion of the data'.[233] It may be worth aligning these two provisions after clarifying their relationship. The retention periods should also be aligned if necessary.

The new Article 18a concerning information processing by Europol in support of specific criminal investigations, must be seen as a 'subset' of Article 18(5a),[234] which will be applied as a first step. This hierarchical relationship between the two articles signifies that the term 'investigative case file' is crucial in determining when Article 18a will be applied. Possible expansions of that definition to data acquired before the investigation, such as when a cyber security authority finds stolen datasets in the course of response to a cyberattack, or in the context of a non-criminal investigation of a legal person for (a criminal) offence and subsequently used in a criminal investigation of a natural person must be carefully considered.[235] An expansive definition of an 'investigative case file' risks frustrating this relationship between the two articles and rendering Article 18a applicable as the first and only step.

---

[227] EDPS, 'Opinion 4/2021' (n 177) para 24.

[228] Commission, 'Europol Impact Assessment Part 1' (n 144) 25.

[229] EDPS, 'Opinion 4/2021' (n 177) para 24.

[230] Commission, 'Europol Impact Assessment Part 1' (n 144) 69.

[231] EDPS, 'Opinion 4/2021' (n 177) para 25.

[232] ibid para 25. See Council, Document 5527/6/21 (23 April 2021) 246.

[233] Council, Document, 5527/6/21 (n 232) 258.

[234] ibid 244.

[235] ibid 249. The definition has already been expanded so that an investigative case file muse be related to an on-going criminal investigation related to one or more Member States. See Council, Document 5388/3/21 (9 April 2021) 22.

In any case, Article 18a provides for a broad derogation from the existing data minimisation and storage limitation safeguards in the Europol Regulation, which might in practice undermine the existing system of checks and balances with regard to personal data processing by the agency. The potential impact of the proposed measure is recognised in the Impact Assessment accompanying the proposal and therefore the provision is construed as a 'narrow and justified exception'[236] and will be applied on an exceptional basis. In the same vein, Recital 18 of the proposal foresees two parallel assessments of the necessity and proportionality of the processing of the investigative file by Europol, carried out by the respective Member State and by the agency. However, these important safeguards remain only in the Recitals and are not reflected in the text of Article 18a, which mentions that there must be a necessity test without explicitly imposing obligations on the Member States.[237] Furthermore, it is **unclear what criteria would be applied to determine that it is an exceptional and duly justified case—in that respect, the intervention of the EDPS could be foreseen**. As for **the assessment provided by Europol that will have been recorded, it could be sent to the EDPS for their information**.

In addition, as Article 18a is construed as an exception, it must be strictly applied and the existence of a link to an on-going investigation is crucial to establish limits for processing. Therefore, **further expansion of its scope, for example by enabling Europol to analyse large datasets not only to provide operational support, but also for cross-checking under Article 18(2)(a), or by enabling *any* Member State to request Europol to store the investigative case file and the outcome of its operational analysis with the preliminary consent of the Member State, and thus expanding the scope of Article 18a(3), is not in line with the exceptional character of Article 18a.**[238] Both suggestions already appear in the latest versions of the proposal, as examined by the Council.[239]

In addition to the aforementioned challenges, the introduction of additional efficient safeguards is vital in order to prevent the risk of an exceptional provision becoming the rule. In line with the EDPS' recommendations, the Regulation should lay down certain conditions and/or thresholds, such as scale, complexity, type or importance of investigations.[240] These legal safeguards should be further particularised and specified by the Management Board of Europol in accordance with Article 18a(2). The processing of personal data under the derogation in Article 18a should in all cases be compliant with the general principles and obligation of Chapter IX of Regulation (EU) 2018/1725. At the time of writing, these issues have not been discussed.

Finally, the rules foreseen in Article 18a(4) as regards the involvement of the EDPS in cases where an investigative case file has been submitted by a third country merit some attention, as this provision has been criticised by Member States as regards the need to delimit the supervision of the EDPS.[241] In particular, whereas the negotiated text retains the requirement that the EDPS is informed about such submissions, the possibility that the EDPS could essentially veto the processing of the data if there are preliminary indications that such data is disproportionate has been removed. It is regrettable that such a provision that would enhance Europol's supervision and transparency has been met with scepticism, not least because certain countries from which Europol may receive investigative case files do not have an adequate level of data protection law and, therefore, it must be ensured that an adequate quality check takes place—the EPDS is well placed to provide such independent and objective assessment. In any case, it should be further required that if there are preliminary indications that such data is disproportionate or collected in violation of fundamental rights, Europol shall not only refrain from

[236] Commission, 'Europol Impact Assessment Part 1' (n 144) 51.

[237] EDPS, 'Opinion 4/2021' para 28. For similar questions see Council, Document 5527/6/21 (n 232) 245.

[238] For such suggestions see Council, Document 5527/6/21 (n 232) 247, 249-250, 253, 259.

[239] Council Document 5388/4/21 (23 April 2021) 28.

[240] EDPS, 'Opinion 4/2021' (n 177) para 29.

[241] Council, Document 5527/6/21 (n 232) 245, 250, 273.

processing the data but also *delete* that data.[242] Finally, the last sentence of Article 18a(4) that data will be shared within the EU is also vital, because, as already mentioned, the level of data protection in third countries from which Europol may receive information may not provide an adequate level of data protection and, as far as is possible, it must be ensured that products of Europol's analysis are not further disseminated by third countries to their own partners.[243]

3.4. Strengthening Europol's role on fostering research and innovation

3.4.1. Calls for an increased role of Europol in research and innovation

Another area where the Commission proposal aims for the agency to acquire a key role is research and innovation so as to support Member States to battle the challenges of criminal exploitation of advanced technologies. Law enforcement authorities face difficulties in detecting and investigating crimes carried out with the support of modern technologies, such as encryption; however technological developments enable them to access tools, particularly Artificial Intelligence (AI), to counter emerging threats. However, not all Member States are able to fully exploit the opportunities of new technologies for fighting crime and terrorism and to overcome the challenges posed by the use of these technologies by criminals and terrorists, given the investment, human and financial resources and skills this requires.[244]

Consequently, and in line with the Declaration of the Home Affairs Ministers of the EU on 'Ten points on the Future of Europol',[245] this thematic block is concerned with the enhancement of the agency's capabilities to harness the potential of technological innovation for law enforcement purposes. Already since October 2019, the Justice and Home Affairs (JHA) Council called for 'the creation of an innovation lab at Europol which could act as an observatory for the creation of new technological developments and drive innovation, including by developing common technological solutions for member states in the field of internal security'.[246] Similarly, the European Parliament in its Resolution of December 2018 called 'for the active involvement of EU agencies such as Europol and CEPOL in EU security research projects'.[247] However, even though Europol has established the Innovation Lab[248] aimed at supporting investigators and law enforcement agencies in making the most of emerging technologies, Europol does not have a mandate to support Member States in fighting serious crime and terrorism by fostering research and innovation and using the results of research relevant for law enforcement, including safeguards with respect to ethical issues and fundamental rights.

3.4.2. Expansion of Europol's tasks on research and innovation

In light of the above, the proposal provides a series of reforms in the Europol Regulation as regards the agency's task to assist the Commission and Member States in identifying, developing and using new technologies for law enforcement purposes. In particular, the rules of Article 4 are expanded so that the agency can 'proactively monitor and contribute to research and innovation activities relevant to

[242] ibid 248.

[243] ibid.

[244] Commission, 'Europol Impact Assessment Part 1' (n 144) 30.

[245] Council, 'Declaration of the Home Affairs Ministers' (n 6) pt 6.

[246] Council, Document 12837/19 (7-8 October 2019).

[247] European Parliament 'Resolution of 18 December 2018 on findings and recommendations of the Special Committee on Terrorism' (P8_TA(2018)0512).

[248] Europol, 'Written contribution to JPSG The Europol Innovation Lab - May 2020', which may be found here <https://www.europarl.europa.eu/cmsdata/208046/Europol%20Contribution%20for%20Electronic%20exchange%20-%20Europol%20Innovation%20Lab.pdf> accessed 3 May 2021.

achieve the objectives set out in Article 3, support related activities of Member States, and implement its research and innovation activities […], including the development, training, testing and validation of algorithms for the development of tools'.[249] Emphasis is on the new technological solutions based on AI, whereby the agency shall play a key role in promoting 'ethical, trustworthy and human centric artificial intelligence subject to robust safeguards in terms of security, safety and fundamental rights'.[250] Furthermore, Europol will assist the Commission in identifying key research themes and drawing up and implementing the EU framework programmes for research and innovation activities that are relevant to achieve its objectives. In cases where Europol draws up and implements an EU framework programme, the agency shall not receive any funding from that programme.[251] The agency will also support the screening of specific cases of foreign direct investments in the EU (pursuant to Regulation (EU) 2019/452)[252] that concern undertakings providing technologies used or being developed by Europol or by Member States for the prevention and investigation of crimes covered by Europol's mandate on the expected implications for security.[253]

According to the proposal, Europol will not merely provide support to the EU security research programme, the Innovation Lab and Europol's support to the innovation hub,[254] but will be involved in research activities. In particular, pursuant to revised Article 18, the agency will also be enabled to process personal data for research and innovation matters for the development, training, testing and validation of algorithms for the development of tools.[255] This option has been preferred to address the need for an EU-level capacity to train, test and validate algorithms for the development of tools, including AI-based tools for law enforcement.[256] In addition, a new provision is inserted in that article prescribing that the processing of personal data for the purpose of research and innovation shall be performed by means of Europol's research and innovation projects with clearly defined objectives, duration and scope of the personal data processing involved, in respect of which additional safeguards will apply, as set out in the new Article 33a.[257] The latter lays down a series of rules on how personal data should be processed for research and innovation purposes, in particular:

1. Any project shall be subject to prior authorisation by the Executive Director, based on a description of the envisaged processing activity setting out:
    a. the necessity to process personal data, such as for exploring and testing innovative solutions and ensuring accuracy of the project results;
    b. a description of the personal data to be processed;
    c. a description of the retention period and conditions for access to the personal data;

[249] Commission, 'Europol proposal of 2020' (n 8) art 1(2)(a)(iv). See recital 37.

[250] ibid recital 38.

[251] ibid art 1(2)(d). See new art 4(4a). Also see recital 11.

[252] Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union [2019] OJ L791/1.

[253] Commission, 'Europol proposal of 2020' (n 9) art 1(2)(d). See new art 4(4b). Also see recital 12.

[254] This is the case with the EBCG/Frontex. See Regulation (EU) 2019/1896 Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624 [2019] OJ L 295/1, art 66.

[255] Commission, 'Europol proposal of 2020' (n 8) art 1(5)(a)(ii). See new art 18(2)(e).

[256] Commission, 'Europol Impact Assessment Part 1' (n 144) 55.

[257] Commission, 'Europol proposal of 2020' (n 8) art 1(5)(b). See new art 18(3a).

d. a data protection impact assessment of the risks to all rights and freedoms of data subjects, including of any bias in the outcome; and

e. the measures envisaged to address those risks.

2. The Management Board and the EDPS shall be informed prior to the launch of the project.

3. Any personal data to be processed shall be temporarily copied to a separate, isolated and protected data processing environment within Europol for the sole purpose of carrying out that project, and only authorised staff of Europol shall have access to that data.

4. Any personal data processed shall not be transmitted, transferred or otherwise accessed by other parties.

5. Any processing of personal data shall not lead to measures or decisions affecting the data subjects.

6. Any personal data processed shall be deleted once the project is concluded or the personal data has reached the end of its retention period.

7. The logs of the processing of personal data shall be kept throughout the duration of the project and for an additional year, solely for the purpose of, and only as long as necessary for, verifying the accuracy of the outcome of the data processing.

8. Finally, the agency shall keep a complete and detailed description of the process and rationale behind the training, testing and validation of algorithms to ensure transparency and for the verification of the accuracy of the results.

3.4.3. Lack of clarity and insufficient data protection safeguards

Europol will acquire a pioneering role in shaping the future of law enforcement tools. From the outset, it must be clarified how the term 'innovation activities' is being defined and used. As the EDPS has stressed in his Opinion on the European Strategy of Data, the definitions and scope of key concepts related to research and innovation are not provided. [258] This approach may blur the boundaries between public interest, academic freedom and private gain and create uncertainty that may have an impact on the protection of fundamental rights. The revision of the Europol Regulation is an opportunity to clarify the scope of such concepts and ensure consistency in the terminology used across legal instruments in data protection law.[259]

It is possible that when developing new technologies **extensive processing of large quantities of personal data** may be required, for example to create and test algorithms or for encryption, which are available to Europol. Expanding the processing activities of Europol constitutes a limitation of the rights to respect for private life (Article 7 of the Charter) and protection of personal data (Article 8 of the Charter). The potential impact of the processing of personal data in the development of algorithms to the principle of non-discrimination (Article 21 of the Charter) must also be taken into account. Therefore, it must be ensured that such processing is in line with the principles of necessity and proportionality, in accordance with Article 52(1) of the Charter. In that respect, it is recalled that in Opinion 1/15 on the EU/Canada PNR Agreement 'the systematic use of [PNR] data for the purpose of verifying the reliability and topicality of the pre-established models and criteria […] or of defining new models and criteria […] [must] not exceed the limits of what is strictly necessary'.[260] In a similar vein,

[258] EDPS, 'Opinion 3/2020 on the European Strategy of Data' (16 June 2020) para 40.

[259] Also see Council, Document 5527/4/21 (n 178) 75.

[260] Opinion 1/15 ECLI:EU:C:2017:592, para 174.

the use of operational personal data, lawfully collected and stored by Europol to develop tools and provide solutions to facilitate the fight against serious crimes and terrorism, could be justified, if accompanied by efficient and appropriate safeguards.[261]

The addition of new Article 33a is a welcome development, as it includes concrete safeguards. These safeguards will constitute *lex specialis*, applicable to Europol as regards the processing of personal data for scientific purposes and, therefore, Article 13 and Chapter IX of Regulation (EU) 2018/1725, which impose strict limitations to the use of operational data, will not be applicable. That said, as the EDPS has noted, the proposed list of safeguards is the minimum and not exhaustive and, therefore, there is room for improvement, so as to bring the Europol Regulation as close to the prescriptions with Regulation (EU) 2018/1725 as possible. One key safeguard to be included is that the processing of personal data for research and innovation should take place **only if needed in order to reach the objectives of the project**.[262] Another important issue is, as the processing of personal data will involve the use of **real operational data**, **to enable the use of synthetic, anonymised or pseudo-anonymised personal data where possible**, which is mentioned in Article 13 of the Regulation (EU) 2018/1725. Whether the **processing of special categories of personal data, which are sensitive in nature, is also permitted for research and innovation purposes is also unclear** and the wording of Article 33a does not explicitly exclude the processing of special categories of personal data. However, the Impact Assessment accompanying the Europol proposal specifically excludes the processing of such data.[263] This approach is in line with Article 76 of Regulation (EU) 2018/1725, which permits the processing of 'only where strictly necessary for operational purposes'. Therefore, **it is necessary that the processing of special categories of personal data is explicitly excluded. If, however, Europol would be permitted to process special categories of personal data appropriate safeguards must be in place on the purpose for processing, the actors that would have access to that sensitive data and the accountability framework**.[264]

Furthermore, **other principles of data protection law not featuring in Article 33a should be taken into account, in particular the principles of data minimisation, data quality and privacy by design and by default**. Indeed, if low quality data are used in the development of algorithms for example, the higher the risk of non-discrimination. As it is mentioned in the Impact Assessment, 'whereas it may be challenging to assess the quality of all data used for building algorithms, it is essential to collect metadata and make quality assessment of the correctness and generalisability of the data'.[265] Moreover, and in line with the comments from the EDPS, **the scope of the research and innovation activities should be further refined by specifically and concretely linking the activities with the tasks of Europol** and clarifying their scope in a binding document, for instance adopted by the Management Board of Europol, which could be subsequently updated, if necessary.[266] That **binding document should be available to the EDPS prior to the launch of each project for information** and consultation and the EDPS should be informed every time the document is updated, as appropriate. Finally, **the one-year retention period of the logs may not be sufficient for data protection purposes and therefore logs could also be kept for an additional period**, **so as to**

[261] EDPS, 'Opinion 4/2021' (n 177) ft 22.
[262] Council, Document 5527/4/21 (n 178) 51.
[263] Commission, 'Europol Impact Assessment Part 1' (n 144) 75.
[264] EDPS, 'Opinion 3/2020' (n 258) para 40.
[265] Commission, 'Europol Impact Assessment Part 1' (n 144) 76.
[266] EDPS, 'Opinion 4/2021' (n 177) para 33.

enable the EDPS to conduct supervision and audits,[267] unless the EDPS would be required to conduct their supervision within a year from the completion of a project.

Another issue that merits further exploration is the extent to which the Commission proposal links to the EU Internal Security Strategy 2020-2025, which envisaged 'the creation of a European Innovation hub for internal security that would seek to deliver common solutions to shared security challenges and opportunities, which Member States might not be able to exploit alone'.[268] This hub would also work with the EBCGA/Frontex, CEPOL, the European Union Agency for the Operational Management of Large-Scale IT Systems (eu-LISA) and the Joint Research Centre. However, nowhere in the proposal is there a reference to the hub and it thus appears that Europol will get the lion's share, if not the monopoly, in supporting the Member States in developing technological tools for law enforcement. Furthermore, as Europol will support the Commission in identifying research themes, the agency is essentially envisaged to become the primary agenda-setter in research and innovation, though it operates within a framework of other agencies in the internal security domain.[269] Furthermore, this relationship between the Commission and Europol may become problematic and undermine the independence of the agency.[270] Similarly, the relationship between Member States' efforts in similar research and innovation must be further defined so that efforts are coordinated, synergies are created[271] and duplication is avoided.[272] In such case, additional safeguards as regards access to the personal data processed by Member States are also necessary and have been added during negotiations by the Council.[273] Consequently, the Council has further emphasised on the need for cooperation with relevant networks of Member States' practitioners and other agencies to drive innovation and foster synergies, within their respective mandates.[274] This is in line with the European Parliament Resolution, as mentioned earlier, which did not provide Europol with an exclusive role in promoting research and innovation.

Finally, the potential involvement of Europol in the screening of specific cases of different investments into the EU concerning undertakings that provide technologies used or developed by Europol or by Member States for the prevention and investigation of crimes has received some attention. Some Member States wish to proceed with this reform subject to amendments (wishing to involve Asset Recovery Offices and the ENUs),[275] whereas many others question whether this task is within the agency's mandate,[276] or whether it creates a conflict of interest.[277] Regulation (EU) 2019/452 establishes a framework for the screening of foreign direct investments into the EU that provides Member States and the Commission with the means to address risks to security or public order in a comprehensive manner and enables the adoption of restrictive measures in relation to foreign direct investment on security and public order grounds. However, public order is not included within Europol's mandate. It is also unclear how Europol would support such screening, as Regulation (EU) 2019/452 does not refer to the role of Europol and such screening is conducted by Member States at the national level, without

[267] Council, Document 5527/4/21 (n 178) 71.
[268] Commission, 'Communication on the EU Security Union Strategy' (n 5).
[269] Council, Document 5527/4/21 (n 178) 86-88, 95.
[270] ibid 92.
[271] For example with the European Network of Law Enforcement Technology Services (ENLETS).
[272] Council, Document 5527/4/21 (n 178) 57.
[273] ibid 71, where Member States ask for access. Also see Council, Document 5388/2/21 (n 179) 42.
[274] Council, Document 5388/2/21 (n 179) recital 37.
[275] Council, Document 5527/4/21 (n 178) 47.
[276] ibid 59.
[277] ibid 17.

necessarily the involvement of law enforcement authorities. As a result, in later drafts of the proposal, this task has been deleted.[278]

3.5. Enabling Europol to register alerts into SIS

One of the most controversial reforms involves the expansion of Europol's tasks to enable the agency to register alerts into SIS. In that respect, a separate Commission proposal has been adopted[279] providing amendments to Regulation (EU) 2018/1962 on the establishment, operation and use of SIS in the field of police cooperation and judicial cooperation in criminal matters. [280]

3.5.1. The relationship between SIS and Europol

Operational since 1995, the overarching purpose of SIS is to ensure a high level of security in the Schengen area by facilitating both border control and police investigations.[281] To these ends, SIS contains alerts on various categories of persons and objects. In connection with each alert, SIS initially stored basic alphanumeric information—such as name, nationality, the type of alert and any specific objective physical characteristics.[282] However, the pressing need to develop a second generation SIS (SIS II), so as to accommodate the expanded EU family after the 2004 enlargement, was seen as an opportunity to insert new functionalities into the system.[283] In 2018, the SIS legal framework underwent another revision primarily with a view to adding certain categories of alerts.[284] According to the current rules, SIS stores alerts on persons wanted for arrest and extradition,[285] missing persons, or vulnerable persons who need to be prevented from travelling,[286] persons sought to assist with a judicial procedure,[287] persons or objects subject to discreet, inquiry or specific checks,[288] objects sought for the purpose of seizure or their use as evidence in criminal proceedings,[289] and unknown wanted persons.[290]

[278] Council, Document 5388/2/21 (n 179).

[279] Commission, 'SIS proposal' (n 16).

[280] Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU [2018] OJ L312/56.

[281] See Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders [2000] OJ L239/19 (CISA), art 93.

[282] CISA, art 94.

[283] Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) [2006] OJ L381/4; Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) [2007] OJ L205/63.

[284] Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals [2018] OJ L312/1; Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006 [2018] OJ L312/14; Regulation 2018/1862 (n 280).

[285] Regulation (EU) 2018/1862, arts 26-31.

[286] Regulation (EU) 2018/1862, arts 32-33.

[287] Regulation (EU) 2018/1862, arts 34-35.

[288] Regulation (EU) 2018/1862, arts 36-37.

[289] Regulation 2018/1862, arts 38-39.

[290] Regulation 2018/1862, arts 40-41.

In addition, SIS stores alerts on third-country nationals subject to return procedures,[291] or to be refused entry or stay in the Schengen area.[292]

SIS has been subject to revisions on numerous occasions, whereby with every reform Europol has benefited from further access to additional alert categories. In the aftermath of the 9/11 terrorist events, the then SIS legal framework was reformed to enable Europol and Eurojust to have 'read only' access to specific types of alerts entered by Member States.[293] Following the latest reform of the SIS legal framework, Europol has 'read-only' access to all categories of alerts.[294]

3.5.2. Limits in information exchanges via SIS

Currently there exist limits in the sharing of information from third countries or organisations on persons who have been suspected or convicted of terrorist offences or other crimes in that such information does not always reach front-line officers, that is police officers and border guards, in the Member States. The prime—and arguably the *only*—example mentioned in the SIS proposal and the Impact Assessment accompanying the Europol proposal concerns the ongoing efforts to detect foreign terrorist fighters on which 'remain a major common security challenge'[295] and necessitate enhanced and timely cooperation and information sharing among Member States, with Europol and other relevant EU actors. However, although Europol has information from third countries and organisations which enters into its own information systems it is not accessible by front-line officers. Approximately 1,000 non-EU foreign terrorist fighters, 'provided by trusted third countries to Europol and individual Member States', have not been inserted into SIS.[296] If no alerts are issued, then border guards may not detect them when they seek to enter the EU, or when police officers check them within the territory of the EU.

However, Member States are not always able to enter information from third countries or international organisations on foreign terrorist fighters into SIS either because such data may have been shared with Europol only, or because even if a Member State receives the information on suspects and criminals directly from the third country or via Europol, it might not be able to issue an alert on the person concerned due to restrictions in national law (e.g. the need to establish a link to national jurisdiction), or because the Member State may not have the means to sufficiently analyse and verify the received information.[297] In turn, though Europol has the means of analysing the information, including on persons involved in organised crime (e.g. drugs trafficking) or serious crime (e.g. child sexual abuse), front-line officers do not access Europol's information systems and the agency does not have the power to record alerts in SIS. Instead, solutions are currently found through cooperation between Europol and Member States whereby the former encourage the latter to issue alerts in SIS, a non-transparent practice that raises legal concerns on responsibility and liability. It also causes operational difficulties,

[291] Regulation 2018/1860, art 3.

[292] For an analysis see Niovi Vavoula, Immigration and Privacy in the Law of the European Union; The Case of Information Systems (Brill Nijhoff, forthcoming 2021) ch 2. Also see Evelien Brouwer, 'Schengen's Undesirable Aliens' in Paul Minderhoud, Sandra Mantu and Karin Zwaan (eds), *Caught in between Borders - Citizens, Migrants, Humans: Liber Amicorum in honour of prof. dr. Elspeth Guild* (Wolf Legal Publishers 2019).

[293] Council Decision 2005/211/JHA of 24 February 2005 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism [2005] OJ L68/44, art 1(9).

[294] Regulation 2018/1862, art 48.

[295] Council, Document 8868/20 (16 June 2020). See Council, Document 9680/18 (4 June 2018), which states that information foreign terrorist fighters should be uploaded to European systems and platforms.

[296] Commission, 'SIS proposal' (n 16) 1.

[297] ibid 2.

as in case of a 'hit' on such an alert issued, the underlying analysis held by Europol is needed for a follow up.[298]

3.5.3. Entry of SIS alerts by Europol

Article 1(2)(a)(iv) of the Europol proposal amends Article 4 of the Europol Regulation with a view to enabling the agency to enter data into SIS, following consultation with the Member States and under authorisation by the Executive Director. This alert should concern the suspected involvement of a third-country national in an offence in respect of which Europol is competent and of which it is aware on the basis of information received from third countries or international organisations.[299]

Furthermore, the SIS proposal prescribes the establishment of a new alert category specifically for Europol will be established, in order to provide information directly and in real-time to front-line officers.[300] The proposal foresees that Europol will be able to issue **'information alerts' on suspects and criminals as a new alert category in SIS**, to be issued exclusively by Europol in specific cases and circumstances. In particular, such alerts will be issued based on Europol's analysis of information from third countries or international organisations received in accordance with Article 17(1)(b) of the Europol Regulation, in relation to crimes which fall within the agency's mandate and only on third-country nationals, excluding those who are beneficiaries of free movement rights. Alerts may be issued in respect of third-country nationals who are suspected of having committed or taken part in a criminal offence in respect of which Europol is competent, or who have been convicted of such an offence; or persons regarding whom there are factual indications or reasonable grounds to believe that they will commit criminal offences in respect of which Europol is competent.[301]

Europol is obliged to undertake a series of steps prior to the entry of the alert in SIS:

- Europol must have analysed the information received and carry out a detailed individual assessment, for example by cross-checking it against other available information, so as to verify its accuracy and to get the 'bigger picture'.[302] This will be to check 'the reliability of the source and the accuracy of the information'.[303]
- *If necessary*, Europol will have to carry out further information exchange with the third country or international organisation involved and has to assess whether entering the alert is necessary for achieving its objectives.[304]
- Europol will have to verify that entering the alert is necessary for achieving Europol's objectives.[305]
- Europol will have to check that there is no existing alert in SIS on the same person.[306]
- Europol will have to share the information collected on the person concerned with all Member States and carry out a prior consultation in order to confirm that no Member State intends to enter the alert themselves based on the information collected by Europol, and that Member

[298] Commission, 'Europol Impact Assessment Part 2' (n 144) 91.
[299] Commission, 'Europol proposal of 2020' (n 8) recital 8.
[300] Commission, 'SIS proposal' (n 16) 3.
[301] Commission, 'SIS proposal' (n 16) art 1(4). See new art 37a(2).
[302] ibid recital 8.
[303] ibid article 1(4). See new art 37a(3)(a).
[304] ibid.
[305] ibid art 1(4). See new art 37a(3)(b).
[306] ibid recital 9 and art 1(4). See new art 37a(3)(c).

States do not object to the alert being entered by Europol.[307] These rules are intended to ensure that if a Member State considers that they have sufficient information and grounds to fulfil the requirements of Regulation (EU) 2018/1862, as well as their national provisions for entering the alert themselves, then they have the possibility to do so and that alert takes precedence. In this case, Member States have the possibility to determine the relevant alert category available to them, based on Regulation (EU) 2018/1862, and issue an alert. Member States also have the possibility to object to the alert being entered by Europol in justified cases, in particular if their national security so requires or when it is likely that the alert would represent a risk for official or legal inquiries, investigations or procedures or if they obtain new information about the person who is the subject of the alert which changes the assessment of the case.

- In order to ensure data protection monitoring by the EDPS, Europol shall keep detailed records relating to the entry of the alert in SIS and the grounds for such entry that permit verification of compliance with the substantive and procedural requirements.[308]
- All Member States have to be informed of the entry of the alert in SIS through the exchange of supplementary information.[309]

In case of a 'hit', the purpose of the new alert is to inform the front-line officer that Europol holds information giving grounds to consider that the person is intending to commit, or is committing, one of the offences falling under Europol's competence, or that an overall assessment of the information available to Europol gives reason to believe that the person may commit such an offence in the future.[310] In terms of the action to be taken upon identifying the person against whom an alert is issued, the proposed rules are reminiscent of the action taken in cases of alerts on discreet checks, pursuant to Article 37(1) of Regulation (EU) 2018/1862. In fact, the issuance of alerts by Europol by making use of Article 36 of Regulation (EU) 2018/1862 had been considered as an option due to the apparent similarities. However, alerts on discreet check alerts may be issued by national competent authorities, in the context of criminal investigations or to prevent threats to public or national security, under conditions also laid down in national law. In the present case, all of the procedural rules and requirements for entering an alert will be regulated under EU law.

The front-line officer will have to report immediately that a 'hit' has occurred to the National Bureau for Supplementary Information Request at the National Entries (SIRENE) and would indicate the place, time and reason for the check carried out.[311] Then the National SIRENE Bureau will communicate this information to Europol.[312] The SIS proposal foresees no further obligation on the Member State, for example to discreetly check the person under alert and collect a set of detailed information, apart from this reporting. Nevertheless, the Member State executing the alert will be provided the discretion to determine, on a case-by-case basis, including based on the background information received from Europol, whether further measures need to be taken with regard to the person *under national law* and at the full discretion of that Member State.[313] Similarly to other alert categories, the proposal lays down the retention period for alert entered by Europol as one year. Finally, an alert entered by Europol in SIS should be deleted, particularly if the person who is the subject of the alert no longer falls under the

[307] ibid recital 9 and art 1(4). See new art 37a(3)(d).

[308] ibid recital 10 and art 1(4). See new art 37a(4). Elsewhere in the proposal the EDPS should conduct an audit at least every four years. Art 1(5)(d). See new art 37b(d).

[309] ibid art 1(4). See new art 37a(5).

[310] Commission, 'SIS proposal' (n 16) 11.

[311] ibid art 1(4). See new art 37b(1).

[312] ibid art 1(4). See new art 37b(2).

[313] ibid art 1(4). See new art 37b(1)(b).

scope of this alert category, a Member State objects to the insertion of such alert, another alert is entered in SIS by a Member State or if Europol becomes aware that the information received from the third country or international organisation was incorrect or was communicated to Europol for unlawful purposes, for example if sharing the information on the person was motivated by political reasons.[314]

3.5.4. Significant fundamental rights and operational challenges

This reform is particularly controversial, thus diverging approaches have emerged with certain Member States[315] having substantial reservations as to the possibility for Europol to enter alerts into SIS, and others broadly supporting the Commission proposals possibly with some amendments.[316]

From the outset, it is noteworthy that this is not the first time that ideas concerning the possibility of Europol having a more active role in the operationalisation of SIS feature in policy documentation, but this is the first time they make their way to legislation. At the time when the SIS rules were subject to revision in the aftermath of the 9/11 events, it was advocated that Europol's access to SIS should take place in two phases, whereby under the first phase all information in SIS could be accessed by the agency, including partial downloading of data in order to carry out analyses and statistical studies, and under the second phase Europol would be enabled to update the system by adding, deleting and modifying information.[317] With Europol having access to all SIS alerts, it is arguable that Europol's role in the operation of SIS is entering its second phase.

Overall, the possibility of enabling Europol to record alerts in SIS presents **numerous legal and operational challenges as regards the nature of SIS and the agency, quality of information, fundamental rights of individuals and possible conflict with national law and investigations**.

This reform marks another important shift in the operation of the agency in two respects; first, in the identity of SIS as an information system exemplifying and fostering mutual trust among Member States that populate it with alerts for which they are responsible, whereas Europol is limited to a 'read-only' access to all alert categories. In that respect, significant questions are raised as to **whether Europol's mandate as an EU agency aimed to support Member States in investigations supports this shift, which essentially places Europol, whose work is covered with some secrecy and non-transparency, on an equal footing with Member States.** It will result in **expanding mutual recognition of alerts to those entered by Europol**. This approach further raises fundamental questions as to whether the principle of mutual trust is to some degree extended to *Europol and its partners from outside the EU* with different legal systems, fundamental rights protection, procedural safeguards and adherence to the rule of law and on whether Europol can and should be allowed to operate as a Member State. In addition, this new paradigm sits at odds with remarks in the previous section about the reluctance on behalf of Member States to share their information with Europol and appears rather premature to say the least.

Whereas the proposal foresees that Europol would have to undertake a series of steps to safeguard the reliability and accuracy of the information received, **it is questionable whether—and how—Europol will handle the issuance of alerts and analyse information received from third countries or organisations so as to undertake a meaningful quality check**. This check is mandated under Article 59 of Regulation (EU) 2018/1862. It must be recalled that Europol has signed a series of operational agreements with third countries, including the United States (US), which are still in place and on the

[314] ibid recital 11.

[315] Such as France, Greece, Malta, Netherlands, Belgium and Germany.

[316] Such as Austria, Czech Republic, Slovakia. See Council, Document 7732/21 (n 316).

[317] Council, Document 5970/02 (8 February 2002).

basis of which the agency receives information from those partners. However, the existence of these agreements does not automatically signify that those countries are trustworthy sources of information. At the same time, Europol has a series of informal arrangement with EU bodies and missions.[318] Overall, **it is uncertain which criteria will be employed to qualify specific third countries as trusted and to verify the reliability and accuracy of information. It is also uncertain whether Europol could provide such assessment given the potentially large quantity of data involved, which must be dealt with on a case-by-case basis**. This could potentially be more problematic in cases where more than two countries are involved, such as when a third country has information about an individual who does not hold the nationality of that country and resides in another third country (e.g. information from the US on an Algerian foreign terrorist fighter in Syria). In such cases, it may be highly difficult for Europol to conduct such verifications, but **there are no specific indications as to when Europol will halt the procedure and decide not to enter an alert**. In 2019, Europol accepted almost 12,000 operational contributions from third countries, and there were over 700,000 objects recorded in the Europol Information System that stem from Europol's analysis of data it received from third countries.[319] However, more information is needed as to whether and how Europol rejected information from third countries or conversely whether following its own analysis Europol incorporates *en masse* information from third countries and organisations. Overall, the quality control constitutes an important issue in this process, which may have significant implications, as outlined further below.

Co-opting Member States in a (joint) verification process through consultation to some extent will enable Member States to use their own resources to verify the reliability of the alert and decide whether they would be willing or able to enter an alert on their own in case of a specific national interest. In practice, as most Member States under their national laws require the existence of a link between the person concerned and the national territory, this procedure may not be particularly helpful. However, the proposal goes beyond that to essentially **bypass national constraints as regards the entry of SIS alerts** and establish alerts on threats against collective EU internal security without the need for a national interest; in other words, Europol would issue an alert on behalf of all Member States and in the general interest of the EU. The potential misuse of such alerts, whereby the threat that individuals may pose will be first determined by the standards of third countries and transplanted into the EU, is highly problematic as the threat may be remote.

The aforementioned difficulties in assessing the reliability of the information provided by third countries or organisations are coupled with the **limited operational value of entering such alerts into SIS**. On the one hand, it has been argued that from an operational perspective the existence of a substantial security gap is unclear; as front-line officers have found difficulties to identify concrete situations in which it would be useful for them to receive certain information they need and are supposedly not receiving.[320] On the other hand, Europol alerts are 'information alerts' and therefore in cases of a 'hit' national police officers and border guards are merely required to inform Europol and decide on the basis of national law whether to take further action. As mentioned above, this type of action mirrors Article 37 of Regulation (EU) 2018/1862 on discreet checks, but with less information to be recorded and with no requirement for the front-line officer to carry out a discreet check. Thus, **the potential further action to be taken by Member States is vague, as well as the responsibility of**

[318] See Valsamis Mitsilegas, 'Extraterritorial Immigration Control, Preventive Justice and the Rule of Law in Turbulent Times: Lessons from the Anti-Smuggling Crusade in Juan Santos Vara, Sergio Carrera and Tineke Strik (eds), *Constitutionalising the External Dimension of EU Migration Policies in Times of Crisis: Legality, Rule of Law and Fundamental Rights Reconsidered* (Edward Elgar 2019).

[319] Commission, 'Europol Impact Assessment Part 2' (n 144) 89.

[320] See Council, Internal Document WK 3974/2021 (19 March 2021).

Member States, which will have to decide on whether and what action should be taken to adequately respond without much clarity about the purpose to be achieved. The mere existence of a 'hit' seems to co-opt Member States and places on them some responsibility to adequately respond. This may lead to wide divergences observed at national level and, consequently, fragmented and uneven implementation. The type of action undertaken by Member States is also unclear, for example a 'hit' could lead a Member State to proactively open **investigations or it may be considered as an open suggestion to assist a third country** in their investigation, even if there may be no clear interest for the Member State where the 'hit' was observed.[321] If so, then SIS is not the appropriate tool for the initiation of investigations and in essence an alert may have the equivalent effect of a request for initiation of investigation, thus expanding and magnifying Europol's powers on that matter. Further issues may occur in cases where a front-line officer takes concrete action on the basis of an information alert which has been entered without appropriate control, in which case they may raise legality concerns that action taken on the basis of a Europol alert may expose them to potential liability, if the individual concerned initiates proceedings against the state. The potential **implications for individuals subject to such alerts are highly important.** These implications are not only data protection and privacy-related ones, but extend to other fundamental rights, such as the prohibition of inhuman and degrading treatment, enshrined in Article 3 of the European Convention on Human Rights (ECHR) and Article 4 of the Charter. **This can be the case when third countries may misuse SIS as a (potentially extraterritorial) monitoring tool for travel movement or where abuses may take place during border controls against third-country nationals on the basis of potentially unreliable information**. Furthermore, without further action taken at national level, the information alert entered by Europol will be ineffective and practically of limited practical use and added value; on the face of it, the proposal does not oblige to halt the entry of suspected terrorists and Member States' authorities may let a suspected terrorist or criminal enter their national territory. However, this raises issues in cases where the information entered was correct and a terrorist offence or a serious crime is committed. In such a case, Europol could 'wash their hands off' and place the responsibility on the Member State in question which failed to adequately respond, which in turn could counter-argue that under the SIS legal framework it was not obliged to take further action. Overall, if there are doubts about the exploitability of the information, national authorities may be very hesitant to further act on an alert. In other words, **national officers are placed between a rock and a hard place; if they do nothing further beyond reporting, there may be a risk for the EU internal security, but if they do act there is a risk of exposure and consequent liability for taking action under Article 72 of the SIS Regulation on the basis of unlawfully recorded information in SIS.** Unless national officers can meaningfully and confidently act on the alert, it is submitted that there is no reason to be made aware of such alerts.

Related to these issues, it is recalled that SIS has already been subject to criticism in relation to the recording of alerts on individuals who should be subject to discreet checks or specific checks (or inquiry checks) in accordance with Articles 36-37 of the Regulation (EU) 2018/1862. It has been reported that alerts on discreet checks have been subject to variable practices by Member States. For example, in France it seems that alerts on discreet checks were registered '*en masse*' as a response to terrorist events that occurred in 2015.[322] Therefore, with SIS already marked by opacity as regards uploading and

[321] ibid.

[322] Lori Hinnant, 'France puts 78,000 security threats in vast police database' (*Associated Press*, 04.04.2018) <https://apnews.com/a1690ac25cea4d5b8d2b622d3fd4e646/France-puts-78,000-security-threats-on-vast-police-database> accessed 3 May 2021. For further analysis of this argument see Niovi Vavoula, 'The European Commission package of ETIAS consequential amendments: Substitute impact assessment (Study for Directorate-General for Parliamentary Research Services (EPRS) of the European Parliament, December 2019).

evaluation of alerts by Member States, which delimits individuals from having access to effective remedies,[323] this reform risks further **undermining the operation and reliability of SIS.**

Finally, **the Explanatory Memorandum accompanying the Europol proposal and the Impact Assessment heavily emphasise on a counter-terrorism rationale to justify the need to enable Europol to enter alerts into SIS**, however **the scope of this reform is much wider, encompassing all criminal offences on which Europol may have third-party-sourced information** and fall within Europol's mandate. This raises concerns about the necessity of enabling Europol to enter alerts to SIS on all offences within its mandate, as there is lack of information on information from third countries and organisations that is available to Europol and could be entered in the system.[324]

3.5.5. Alternative options

In addition to the aforementioned challenges, other solutions should be further evaluated as alternative options.[325] One such solution is the possibility of **making better use of Interpol alerts and notices**, which are (or could be) available to front-line officers.[326] Admittedly, these alerts are not always visible to front-line officers in the Member States and apparently divergences among Member States exist. Some of them apply their own national verification process before making Interpol notices available to front-line officers through their national systems, whereas others do not make such notices available to their front-line officers.[327] However, **it is unclear why improving the availability of Interpol alerts so that these can be better used has not been preferred as an option and why there is limited information on the countries where Interpol alerts are not visible to all front-line officers**.

Another way forward is the **use of an informal Protocol developed by the Terrorism Working Party and endorsed by the Standing Committee on Operational Cooperation on Internal Security (COSI) in November 2020** that sets out a process for evaluating information on suspected foreign terrorist fighters from third countries and possibly entering relevant data in SIS if legal prerequisites on

[323] See Evelien Brouwer, *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System* (Martinus Nijhoff 2008).

[324] Council, Internal Document WK 3974/2021 (n 320).

[325] Council, Document 13037/20 (11 November 2020); See 'The Development of Europol's missions: Non Paper submitted by France and Greece on the creation of alerts in the SIS', as mentioned in Council, Document 7732/21 (n 316). Other alternative solutions are not examined in this section because of their irrelevance. It suffices here to mention that in relation to interoperability, Regulations (EU) 2019/817 and 2019/818 do not alter the access rights and therefore front-line officers, who do not have access to Europol information systems will continue not to have such access. See Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA [2019] OJ L 135/27; Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 [2019] OJ L 135/85. Another alternative that has been proposed concerns the use of Querying Europol's Systems (QUEST), which is a system interface allowing Member States' investigators, criminal intelligence officers and analysts to search and access Europol's databases using their own national information systems. Even if front-line officers would be given access to Europol information system through QUEST, then the information within would not be suitable for use during a border or a police check and is not actionable information. See Council, Internal Document WK 3974/2021 (n 320) 27. Also see Commission, 'Europol Impact Assessment Part 2' (n 144) 78, 96.

[326] Council, Internal Document WK 3974/2021 (n 320).

[327] ibid 4.

national and EU levels are met.[328] This protocol, which arguably has not attracted much attention, entails a seven-step approach with the involvement of Europol, which entails the following steps:

- Europol informs the Presidency, the Member States, the Commission and the EU Counter-Terrorism Coordinator of the list of foreign terrorist fighters and transmits it to Member States (Step 1).
- Europol conducts a first quality check, verifies whether individuals on the list are already inserted into SIS and prepares an updated list enriched with relevant additional information (Step 2).
- Europol informs the Member States on the outcome of the data processing exercise conducted by Europol by forwarding the updated list. On the basis of this updated list, the competent authorities of the Member States will have the opportunity to conduct a quality check of the list and edit the list if necessary (Step 3).
- The list is updated on the basis of comments and national competent authorities establish a voluntary group of Member States who are willing to further process the list, allowing for possible entry into SIS, and allocation of burden sharing (Step 4).
- Participating Member States in the voluntary group process and analyse parts of the list as agreed and, where appropriate, information on foreign terrorist fighters is inserted into SIS. The usual SIS principles regarding individual assessment and conditions for entering alerts are applicable. In such cases, Europol is available for support to the Member States (Step 5).
- Participating Member States' authorities keeps the Presidency informed on progress and provide information on created alerts (Step 6).
- Europol shall ensure that information on hits related to foreign terrorist fighters inserted in SIS is shared in accordance with Regulation (EU) 2018/1862 to the agency's counterparts, thus subject to the consent of the issuing Member State (Step 7).

The Protocol on entering third-country-sourced information in SIS by volunteering Member States is far from perfect due to transparency and legality concerns stemming from its informal character, but in comparison to the Commission's proposal, it carries a series of benefits: it maintains Member States as the leads of SIS alerts[329] and of the quality check of the information—Europol conducts the first quality check, but ultimately Member States process the updated list and make the call as to whether the issuance of an alert is appropriate and which category of alert will be used (e.g. a alert for arrest or a refusal of entry). In that respect, where appropriate, a judicial or administrative decision will be issued in accordance with their national law.

It has been argued by the Commission that the Protocol is a 'temporary, voluntary and *ad hoc* solution that might not be sufficient as a sustainable, long-term solution'. As the Protocol was only agreed in November 2020, a few weeks prior to the adoption of the Europol and SIS proposals, it is questionable why such a significant divergence from the content of the Protocol is foreseen. The proposal does not simply build on the Protocol, but rather entails a paradigmatic shift, which is not inconsequential. From an operational perspective, the Protocol presents a drawback in that when a volunteering Member State enters a SIS alert, the information on a 'hit' is sent back to the Member State that entered the alert which might not have sufficient interest or capacity for further follow up of a case which has no link to

[328] See Council, Document 13037/30 (16 November 2020).

[329] Council, Internal Document WK 3974/2021 (n 320) 3.

its territory.[330] However, Europol can contribute to that work not least because supplementary information cannot be shared with third countries by Member States; it can be done only via Europol.[331] An option to mitigate this concern without altering the architecture of SIS is by making use of Article 48(8) of Regulation (EU) 2018/1862, which requires Member States to inform Europol on terrorism-related alerts.

Finally, in relation to other criminal offences, France has suggested the creation of a mechanism in which Europol would support the Member States in the processing of third country information they should enter into SIS, with subsequent reporting to Europol regarding action taken.[332]

3.5.6. The compromise solution: Europol alerts related to counter-terrorism from 'trusted' countries

Another compromise solution, which has gained support within the Council, is the possibility to delimit the introduction of Europol alerts in SIS in cases related to terrorism-related activities from trusted countries, namely third countries with which Europol has an operational agreement or which are subject to the Commission adequacy decision. At least one Member State would have to request from Europol to record a SIS alert.[333] Firstly, this approach does not alter the finding that essentially Member States could bypass their national restrictions in enabling Europol to enter alerts when they cannot establish sufficient links between the individual concerned and their national territory. Secondly, it is doubtful whether that would be the end of the story. This will be a compromise interim solution and '[a]fter a certain period of time, the use of this instrument can be analysed and evaluated, and then its scope can be extended to include other offenses under Europol's mandate'.[334] Therefore, it is expected that **this reform will serve as the gateway to further expand Europol's powers to enter alerts into SIS in the future**. Thirdly, the qualification of a third country as 'trusted' may raise significant concerns. As stated earlier, the existence of an operational agreement between Europol and third countries cannot be equated with the existence of an adequate level of data protection. It is true that Europol's strategic agreements are more limited in that they allow for the exchange of information, except for personal data, while operational agreements include the issues covered by strategic agreements plus personal data exchanges and thus their use depends on the level of trust in its partners. As Coman-Kund has noted, 'strategic agreements aim to establish formal cooperation with partners whose data protection system or human rights record might be problematic and operational agreements with close partners'.[335] A prime example of an operational agreement of Europol with a third country that raises significant doubts as to whether the partner is trusted is that with the US, which has been criticised for not meeting legal safeguards including on data protection.[336] In particular, the 2002 Supplemental Agreement with the US mentions nothing about the adequate level protection of personal data and is laconic about data protection safeguards. Furthermore, its provisions on liability are unclear and it does not include elaborated provisions on dispute settlement. As a result, the criteria to be used to qualify a third country as 'trusted' are not satisfactory.

---

[330] ibid 21.

[331] ibid.

[332] Council, Document 7732/21 (n 316).

[333] ibid.

[334] Council, Internal Document WK 3974/2021 (n 320) 11.

[335] See Florin Coman-Kund, 'Europol's International Cooperation between 'Past Present' and 'Present Future': Reshaping the External Dimension of EU Police Cooperation' (2018) 2(1) Europe and the World 1, 11.

[336] ibid 13. See Dick Heimans, 'The External Relations of Europol – Political, Legal and Operational Considerations' in Berndt Martenczuk and Servaas van Thiel (eds), *Justice, Liberty and Security: New Challenges for EU External Relations* (VUBPRESS 2008) 385-387.

3.6. Enhancing cooperation with third countries

3.6.1. Exchange of personal data between Europol and third countries

Third countries may hold important information in countering serious crime and terrorism with links beyond the EU territory. Under the current legal framework, as laid down in Article 25(1) of the Europol Regulation and outlined in Section 2.5, the agency may receive personal data from third countries based on: a) adequacy decisions under Directive (EU) 20016/680;[337] b) international agreements under the current Regulation concluded in accordance with Article 218 TFEU; and c) cooperation agreements concluded between Europol and third countries under the previous Europol Council Decision. However, the Commission has not yet adopted an adequacy decision in accordance with Article 36 of the Law Enforcement Directive that would allow for the free transfer of personal data to a third country.[338] Adequacy decisions have been adopted pursuant to Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR),[339] but these do not cover data exchanges in the law enforcement sector which are governed by the Law Enforcement Directive.[340] Furthermore, in June 2018 the Council adopted eight mandates for the Commission to enter into negotiations with priority third countries (Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey) on strengthening the cooperation with Europol,[341] but these have not resulted in conclusion of such agreements. Whereas in one case considerable progress has been made, in the other cases progress is insufficient, either due to political reasons in the third country or because the third countries are not interested in entering into such negotiations.[342] In 2020, the Commission received a mandate to enter negotiations for an agreement with New Zealand.[343]

In addition, Article 25(5) of the Europol Regulation provides derogation to Article 25(1) and states that personal data may be transferred in specific situations, as listed therein, and on a case-by-case basis following authorisation by the Executive Director. Although the Europol Regulation has not undergone proper evaluation, the Impact Assessment notes that the Executive Director has made use of that derogation in two cases, one of which concerns the cooperation with New Zealand in the aftermath of the Christchurch attack in March 2019. There is another derogation, set out in Article 25(6) on the possibility to transfer personal data on the basis of a self-assessment of the adequate level of safeguards and an authorisation by the Management Board, in agreement with the EDPS, which has

[337] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89 (Law Enforcement Directive).

[338] Commission, 'Europol Impact Assessment Part 2' (n 144) 107.

[339] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

[340] The Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay as providing adequate protection. On 30 March 2021, adequacy talks were concluded with South Korea. On 19 February 2021, the Commission launched the procedure for the adoption of two adequacy decisions for transfers of personal data to the United Kingdom, under the GDPR and the Law Enforcement Directive respectively. For further information on adequacy decisions see Commission 'Adequacy decisions'

<https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> accessed 3 May 2021.

[341] For an analysis see 'EU: Warnings over proposed new Europol partners in Middle East and North Africa' (*Statewatch*, 14 May 2018) <https://www.statewatch.org/news/2018/may/eu-warnings-over-proposed-new-europol-partners-in-middle-east-and-north-africa/> accessed 3 May 2021.

[342] Commission, 'Europol Impact Assessment Part 2' (n 144) 107-108.

[343] ibid 108.

not been applied in practice, as 'there are uncertainties around the conditions under which such transfer mechanism can be used'.[344]

In that respect, in July 2020, the European Parliament adopted a Resolution stating that 'cross-border information exchange between all relevant law enforcement agencies, within the EU and with global partners, should be prioritised in order to fight serious crime and terrorism more effectively'.[345] Cooperation with third countries also features in the Declaration of the Home Affairs Ministers of the EU on 'Ten points on the Future of Europol,' where it is highlighted that 'if Europol is to properly fulfil its role as EU criminal information hub, more effective mechanisms must be put in place through which it can exchange information with other third countries'.[346] At the same time, Europol has also expressed an operational need for a less cumbersome regime for the exchange of personal data with third countries, without an adequacy decision or international agreement.[347]

3.6.2. 'Transfers or categories of transfers of personal data'

Against this backdrop, the proposal foresees a (seemingly minor) change in Article 25(5) so that the Executive Director may authorise not only *transfers,* but also *categories of transfers* of personal data to third countries or international organisations in specific situations and on a case-by-case basis.[348] Furthermore, Article 1(11) of the proposal further stipulates the inclusion (rather than the deletion as it is stated by mistake) of a provision according to which a transfer of personal data pursuant to Article 25(5) shall be documented and the documentation shall be made available to the EDPS on request. The documentation shall include a record of the date and time of the transfer, and information about the receiving competent authority, about the justification for the transfer and about the operational personal data transferred.

3.6.3. A small change with far reaching consequences?

This minor difference in the text has already led to operational challenges when Europol applied the derogation to support New Zealand in the investigation of the Christchurch attack. In a footnote of the Impact Assessment it is further explained that for each transfer of personal data a dedicated authorisation, including procedure and justification, was necessary and the actual personal data to be transferred was not known from the outset.[349] The proposed change must be viewed in conjunction with Article 38 of the Law Enforcement Directive, which prescribes derogation to Articles 35-37 of that Directive concerning the rules on transfers of personal data to third countries and uses the same wording allowing a 'transfer or a category of transfers of personal data to a third country or an international organisation' provided that certain conditions are met. According to the Impact Assessment, 'Member States often rely on the derogations for the transfer of personal data' as provided in Article 38.[350] This allows for transfers of a category of personal data, such as *data of persons that are related to the specific crime* where this is necessary for the investigation, while the exact scope of the persons implied might not be known yet at the time when the authorisation for the transfers is sought.[351]

---

[344] ibid 108.

[345] European Parliament, 'Resolution of 10 July 2020 on the European Parliament recommendation to the Council and the Commission concerning the conclusion of an agreement, under negotiation, between the European Union and New Zealand on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the New Zealand authorities competent for fighting serious crime and terrorism'.

[346] Council, 'Declaration of the Home Affairs Ministers' (n 6) pt 9.

[347] Europol, 'Europol's main operational considerations' (n 7).

[348] Commission, 'Europol proposal of 2020' (n 8) art 1(11) and Recital 24.

[349] Commission, 'Europol Impact Assessment Part 2' (n 144) 110.

[350] ibid 109.

[351] ibid 109.

Nonetheless, **it is not clear what exactly is meant by 'categories of transfers'** and how they differ from the 'sets of transfers' as mentioned in Article 25(6). The proposed Recital 24 also refers to a 'group of transfers'. Besides, it is also unclear how this reform will be in line with the requirement of Article 25(5) that transfers should take place on a 'case-by-case basis'.[352] This vagueness may create potential risks for the protection of personal data of the affected individuals, especially if in practice a broad interpretation of the notion is applied by the agency. It may broaden the remit of such transfers from criminal investigations on specific suspects to surveillance activities in general, thus changing Europol's powers. In that respect, it should be noted that the proposal for the Law Enforcement Directive did not foresee that wording and merely referred to a transfer of data.[353] In any case, the Law Enforcement Directive has also not been subject to an evaluation, which is due to take place in 2022. As the information about the 'often use' of the derogation is insufficient, it is necessary to have a clear view of how the derogation has been used, before transplanting that reform to the Europol legal framework takes place. In any case, a clarification on what is meant by categories of transfers is necessary, at least in a Recital. Furthermore, that term must be distinguished from the term 'sets of transfers'.[354]

3.6.4. Further amendments by the Council: Undoing data protection standards

Admittedly, the proposal is more modest in comparison to initial intentions, as laid down in the Inception Impact Assessment,[355] which would bring the Europol Regulation closer to the prescriptions of the Eurojust Regulation[356] and the Law Enforcement Directive.[357] The Inception Impact Assessment considered, as possible options, to transplant the content of Articles 38 of the Data Protection Directive and Article 58 of the Eurojust Regulation to the case of Europol so that additional grounds for transfers could be based on self-assessment, in particular on: (a) the existence of appropriate safeguards in the third country with regard to the protection of personal data in a legally binding instrument; or (b) the existence of appropriate safeguards in the third country with regard to the protection of personal data as assessed by Europol after having ascertained the specific circumstances that apply to the specific transfer.[358]

In the discussions within the Council, Member States have voiced their preference to include these options and thus transplant the wording of the Law Enforcement Directive and the Eurojust Regulation to the Europol legal framework.[359] Therefore, in recent versions of Article 25, this alignment takes the form of an addition of a new provision replicating the two options contained in the Inception Impact Assessment. This approach is highly problematic and should not be accepted for a series of reasons.

Firstly, from an institutional standpoint both policy options create new legal grounds for transfers outside the three already prescribed ones, and, therefore, should be seen as an effort to bypass the legal ground for the transfer of personal data provided by an international agreement on the basis of Article 218 TFEU, and hence of the European Parliament's right to give consent.[360] I**t is necessary to**

[352] Council, Document 5527/4/21 (n 178) 135.

[353] Commission, 'Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data' COM(2012) 10 final. Also see Council, Document 14934/15 (8 December 2015).

[354] EDPS, 'Opinion 4/2021' (n 177) para 37.

[355] Commission, 'Inception Impact Assessment – Europol Regulation' (2020).

[356] Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA [2018] OJ L 295/138.

[357] Inception Impact Assessment 3-4.

[358] Law Enforcement Directive, art 37.

[359] Council, Document 5527/4/21 (n 178) 34, 110, 115.

[360] Commission, 'Europol Impact Assessment Part 2' (n 144) 113-114.

maintain and enhance parliamentary/democratic scrutiny over the agency's international activity as much as possible and this proposed reform constitutes a major step back.

Secondly, it must be reminded that transfer of personal data to third countries constitutes a separate interference with the rights to respect for private life and protection of personal data[361] and, therefore, the rules must ensure that the limitations to the rights in relation to the fight against serious crime and terrorism must apply in so far as it is strictly necessary and proportionate. In that respect, as mentioned in the Impact Assessment accompanying the proposal, such options have already been considered and discarded. The option under (a) was discarded at an early stage because a legally binding instrument for the transfer of personal data to a third country requires an international agreement under Article 218 TFEU.[362] In the case of the Law Enforcement Directive, that legally binding document may be bilateral agreements between a Member State and a third country. As regards the Eurojust Regulation, it remains unclear how this provision referring to a 'legally binding document' could be applied and, as the Impact Assessment states, 'it is therefore not used in practice'.[363] In light of the above, it not possible to determine how this legal ground for transfer may operate in practice and it has been proposed that the legally binding document could be those bilateral agreements which have been concluded by the Member States and implemented in their legal order.[364] This approach raises a series of significant questions as to whether the self-assessment of one Member State and the **conclusion of bilateral agreements with a third country will be essentially recognised by the agency**, **whether different standards that may be applicable depending on whether some Member States have agreements with third countries, as well as questions of potential conflicts in cross-border cases, whereby data concerning one case originating from different countries are to be transferred in a third country and one Member State may have signed a bilateral agreement, but another one may not have**. Further questions are raised as regards who has the ultimate responsibility and upper hand in the self-assessment; is it the Member States and, therefore, a written approval of the Member State that has provided the data must be foreseen as a safeguard, or the Management Board, and in that case it must be explicitly involved in the self-assessment? Moreover, it is unclear how the potential addition of a new rule enabling self-assessment on the basis of appropriate safeguards correlates with the existing derogation under Article 25(6).

Thirdly, the Impact Assessment considered a revision of the derogation based on self-assessment enshrined in Article 25(6), where there would be the adequate level of safeguards and an authorisation by the Management Board, in agreement with the EDPS. That policy option would entail revision of the conditions to provide more clarity and flexibility on how to meet the requirements of adequate safeguards (e.g. the transfers would be targeted to specific purposes and a specific national authority, with conditions attached to be fulfilled by the third country). However, that solution was rightly discarded as this legal ground would not change the fact that international transfers must comply with the CJEU's pronouncements in the case of *Schrems*.[365] It is recalled that in *Schrems* the CJEU provided strict constitutional limits in international transfers, by stressing that in order for a third country to have an adequate level of data protection, the latter must be 'essentially equivalent to that guaranteed in the EU.[366] As a result, with Europol eagerly wanting to have more powers to exchange personal data with third countries, the addition of a legal ground will raise such issues of the potential incompatibility of those transfers with the CJEU's case law. Therefore, a new legal ground not only bypasses the institutional framework, as outlined below, but **undermines the importance of adequacy decisions**

[361] *Weber and Saravia v Germany* (2008) 46 EHRR SE5.

[362] Commission, 'Europol Impact Assessment Part 2' (n 144) 130.

[363] ibid.

[364] Council, Document 5527/6/21 (n 232) 290-291.

[365] Case C362/14 *Maximillian Schrems v Data Protection Commissioner* ECLI:EU:C:2015:650. For an analysis see

[366] Commission, 'Europol Impact Assessment Part 2' (n 144) 113. For an analysis see among others Loïc Azoulai and Marijn Van Der Sluis, 'Institutionalizing Personal Data Protection in Times of Global Institutional Distrust: *Schrems*' (2016) 53(5) Common Market Law Review 1343.

and the procedure for assessing the data protection framework of a third country as adequate. The fact that no adequacy decisions have been adopted in the past years does not mean that the existing safeguards as interpreted by the CJEU should be marginalised; on the contrary, they are a strong testament to the fact that the constitutional threshold is high and third countries' data protection regimes cannot easily meet that. As a result, transfers taking place in blunt disregard of these safeguards may be successfully challenged by the CJEU.

Fourthly, this reform also bypasses and disregards the distinction between operational and strategic agreements according to which only the former enable the exchange of personal data.

Finally, enabling such transfers through the back door may enhance Europol's cooperation with third countries, but it may have a significant impact on the degree of Member States' trust to Europol.

3.7. Strengthening cooperation with the EPPO

3.7.1. Background information

This thematic block concerns the reinforcement of Europol's cooperation with EPPO in the aftermath of the adoption of Regulation (EU) 2017/1939 on the establishment of the EPPO.[367] In accordance with Article 99(1) of the EPPO Regulation, the EPPO's guiding principle is that the agency may establish and maintain cooperative relations with EU entities, international organisations and the competent authorities of third countries, and of Member States which do not participate in enhanced cooperation. Working arrangements may be concluded that they will enable the exchange of strategic information and other technical details of cooperation.[368] As regards the EPPO's relationship with Europol, Article 102(1) of the EPPO Regulation refers to a relationship between the two agencies laid down in a working agreement, which has already been signed and entered into force on 19 January 2021.[369] That article also foresees that where necessary, for the purpose of its investigations, the EPPO *shall be able to obtain, at its request, any relevant information held by Europol*, concerning any offence within its competence, and *may also ask Europol to provide analytical support to a specific investigation conducted by EPPO*. As the Europol Regulation was adopted before the EPPO Regulation, a need to reflect this change has emerged. Besides, this approach on fostering and promoting inter-agency cooperation is in line with the EU Internal Security Strategy, according to which 'relevant authorities at EU level (such as OLAF, Europol, Eurojust and the European Public Prosecutor's Office) should also cooperate more closely and improve the exchange of information'.[370]

3.7.2. Regulating Europol-EPPO cooperation

Against this backdrop, Article 1(8) of the proposal introduces new Article 20a on Europol's relations with the EPPO, to reflect Article 102 of the EPPO Regulation: Europol shall establish and maintain a close relationship with the EPPO within their respective mandates and competences and a working arrangement setting out the modalities of such cooperation will be concluded. It is further proposed that Europol shall actively support the investigations and prosecutions of the EPPO and cooperate with it, in particular through exchanges of information and by providing analytical support.[371] Europol will also take all appropriate measures to enable the EPPO to have indirect access to information provided for the purposes of cross-checking data or operational or strategic analyses on the basis of a hit/no hit system.[372] Article 21 of the Europol Regulation is applied *mutandis mutandis* except for its second

[367] Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office [2017] OJ L283/1 (EPPO Regulation).

[368] EPPO Regulation, art 99(3).

[369] Europol-EPPO, 'Working Arrangement establishing cooperative relations between the European Public Prosecutor's Office and the European Union Agency for Law Enforcement Cooperation'.

[370] Commission, 'Communication on the EU Security Union Strategy' (n 5) 21.

[371] Commission, 'Europol proposal of 2020' (n 8) art 1(8). See new art 20a(2).

[372] ibid art 1(8). See new art 20a(3).

paragraph, which concerns the adoption of working arrangements with Eurojust and OLAF (as a separate Article 20a(1) is proposed). Finally, Europol will report to the EPPO, without undue delay, any criminal conduct in respect of which the EPPO could exercise its competence.[373]

3.7.3. Alignment with the EPPO Regulation

This thematic block does not present controversial matters, as it is meant to update the Europol Regulation following the establishment of the EPPO and the signature of a working arrangement between the two agencies. The primary consideration is to **align the EPPO Regulation with the revised Europol Regulation, as well as to ensure consistency between the cooperation of Europol with the EPPO and the other Agencies in accordance with the working arrangement between the two agencies**. Partly, this has been done by inserting in Article 20a(3) the phrase '*mutandis mutandis*'. However, the Council has also sought to revise the text of Article 20a to reflect that Europol shall support the investigation of the EPPO *following a request by the latter* in accordance with Article 102 of the EPPO Regulation.[374] Furthermore Article 20a(3) on the indirect access to Europol information has been revised to match Article 21(1) on the restrictions to information processing pursuant to Article 19(2).[375] In order to avoid double standards, whereby some rules taken from Article 21 are explicitly stated in Article 20a and others apply *mutandis mutandis*, it is suggested that Article 20a expressly sets out the rules that pertain to Europol's cooperation with the EPPO, or that at least Article 20a refers to the specific paragraphs of Article 21 that are applicable *mutandis mutandis*. Moreover, in reference to 'active support', the activities of the EPPO take their cue from Recital 69 of the EPPO Regulation, but that wording is not found in the body of that Regulation. As for the possibility of Europol to support the EPPO in investigations *and* prosecutions, the working arrangement concluded between the two agencies prescribes that Europol provides assistance to EPPO in criminal investigations.[376]

3.8. Enhancing capacity to request the initiation of criminal investigations

3.8.1. Requesting the initiation of an investigation of cross-border crimes

According to Article 88(1) TFEU, as reflected in Article 3(1) of the Europol Regulation, Europol's mandate is to support and strengthen action by the Member States' law enforcement authorities in preventing and combating not only serious crime affecting two or more Member States and terrorism, but also forms of crime which affect a common interest covered by an EU policy, such as the rule of law, enshrined in Article 2 of the Treaty on the European Union (TEU).[377] These crimes have the potential to affect the Member State where they are committed, as well as all Member States and the foundations of the EU, as they 'transcend boundaries, diffuse and permeate European societies and require a collective response'.[378] The benefits of Europol's role in providing advanced operational support in individual Member States' investigations concerning high profile sensitive cases may be seen, for example after the revelations about the murder of Daphne Caruana Galizia in Malta.[379]

The European Parliament issued a Resolution on that issue in December 2019, reiterating its call for the full and continuous involvement of Europol in all aspects of the murder investigation and called for Europol's involvement to be reinforced as it yields results.[380] Earlier, in July 2019, it called on the Commission to 'strengthen the mandate of Europol so as to enable it to participate more proactively

[373] ibid art 1(8). See new art 20a(4).

[374] Council, Document 5388/4/21 (n 239) 31.

[375] ibid.

[376] Europol-EPPO, 'Working arrangement' (n 369) art 4.

[377] Commission, 'Europol Impact Assessment Part 2' (n 144) 119.

[378] ibid 119.

[379] ibid 120.

[380] European Parliament, 'Resolution of 18 December 2019 on the rule of law in Malta following the recent revelations surrounding the murder of Daphne Caruana Galizia' (P9_TA(2019)0103).

in investigations into leading organised crime groups in Member States where there are serious doubts about the independence and quality of such investigations'.[381] Finally, in July 2020, the European Parliament issued another Resolution requesting 'strengthening Europol's capacity to request the initiation of cross-border investigations, particularly in cases of serious attacks against whistleblowers and investigative journalists'.[382]

Against this background, this thematic block is concerned with clarifying—an expanding—Europol's capacity to request the initiation of an investigation of a crime affecting a common interest covered by an EU policy. This is because, as mentioned in Section 2.3.2, in accordance with Article 6 of the Europol Regulation, the agency may request the initiation of a criminal investigation in a Member State, but only where cross-border cooperation would add value, thus excluding high profile cases that affect the Member State only.

3.8.2. Requesting the initiation of an investigation of a crime affecting a common interest covered by an EU policy

Against this backdrop, Article 1(3) of the proposal amends Article 6(1) of the Europol Regulation which shall read as follows:

> 'In specific cases where Europol considers that a criminal investigation should be initiated into a crime falling within the scope of its objectives, it shall request the competent authorities *of the Member State or* Member States concerned via the national units to initiate, conduct or coordinate such a criminal investigation' [emphasis added].

Recital 14 of the proposal mentions that Europol should be able to request the competent authorities of a Member State to initiate, conduct or coordinate a criminal investigation of a crime, which affects a common interest covered by an EU policy, even where the crime concerned is not of a cross-border nature. Europol should inform Eurojust of such requests. As a result, Europol's tasks to request the initiation of a criminal investigation will be expanded to cover its entire mandate.

3.8.3. Necessity of the reform not demonstrated

This reform has been met with great scepticism by Member States,[383] to the extent that at the time of writing it does not seem that this reform will take place. A large majority of Member States have considered that no further obligation to a Member State to act at the request of Europol should be introduced,[384] as that would be disproportionate,[385] because it arguably encroaches upon national sovereignty. A key consideration in that respect is how and to what extent Article 6(1) of the Europol Regulation has been used in practice, including an assessment on which occasion Member States have refused to initiate criminal investigations, and whether it is appropriate in light of the supportive role of Europol to remove control from judicial authority over the opening of their investigations in cases affecting one Member State only.[386] In view of the lack of an evaluation of the Europol Regulation, there is no statistical data on this issue and therefore the need to amend Article 6 is not demonstrated. This is all the more necessary, having in mind that the concept of 'crime which affects a common interest covered by an EU policy' is particularly vague and may be interpreted in a particularly expansive manner.

---

[381] European Parliament, 'Resolution of 28 March 2019 on the situation of the rule of law and fight against corruption in the EU, specifically in Malta and Slovakia' (P8_TA(2019)0328).

[382] European Parliament, Resolution of 10 July 2020 on a comprehensive Union policy on preventing money laundering and terrorist financing (2020/2686)RSP)).

[383] Council, Document 5527/4/21 (n 178) 10, 24, 29, 50-51,

[384] ibid 97.

[385] ibid 115.

[386] ibid 21, 29.

3.9. Enhancing the data protection framework

3.9.1. Europol's *sui generis* data protection framework

This thematic block concerns the enhancement of Europol's data protection framework given that the Europol Regulation provides for an autonomous data protection regime, which applies specifically to the agency. Section 2.4 has provided a sketch of the applicable set of data protection rules. At the same time, Regulation (EU) 2018/1725, which was subsequently adopted, introduced a distinct chapter with general rules applicable to the processing of operational personal data by EU bodies, offices or agencies when carrying out activities in the fields of judicial and police cooperation. However, EPPO and Europol have maintained their *sui generis* data protection regimes and the rules of Regulation (EU) 2018/1725 are currently not applicable to these agencies.

3.9.2. Progressive alignment with Regulation (EU) 2018/1725

In a nutshell, the changes concerning the strengthening of Europol's legal framework are the following:

1. Article 3 on definitions and Chapter IX of Regulation (EU) 2018/1725 with regard to the processing of operational personal data will become applicable to Europol, while as regards administrative personal data other chapters of that Regulation will apply to Europol.[387] This broadly reflects these changes:
    a. Definitions of 'personal data', 'data subject', 'genetic data', 'processing', 'recipient', 'transfer of personal data', 'personal data breach' and 'the data subject's consent' are thus to be taken from Regulation (EU) 2018/1725.
    b. Article 28 on general data protection principles is deleted.[388]
    c. Articles on data protection by design,[389] notification of a data breach to the EDPS,[390] communication of a data breach to the data subject,[391] rights of access,[392] rectification, erasure and restriction,[393] prior consultation with the EDPS,[394] logging and documentation,[395] the role of the DPO,[396] supervision by national data supervision authorities,[397] the supervision by the EDPS,[398] the right to lodge a complaint with the EDPS[399] and the right to compensation[400] are amended to reflect that Chapter IX of Regulation 2018/125 is applicable to Europol,[401] taking into account the additional points below.
    d. However, a new Article 37a on the right to restriction of processing is introduced, according to which, where the processing of personal data has been restricted under Article 82(3) of Regulation (EU) 2018/1725, such personal data shall only be processed for the protection of the rights of the data subject or another natural or legal person or

[387] Commission, 'Europol proposal of 2020' (n 8) art 1(14). See new art 27a.
[388] ibid, art 1(15).
[389] ibid, art 1(18). See art 33.
[390] ibid art 1(20). See art 34.
[391] ibid art 1(21). See art 35.
[392] ibid art 1(22). See art 36.
[393] ibid art 1(23). See art 37.
[394] ibid art 1(26). See art 39.
[395] ibid art 1(28). See art 40.
[396] ibid art 1(29). See art 41.
[397] ibid art 1(30). See art 42.
[398] ibid art 1(32). See art 43.
[399] ibid art 1(35)(a). See art 47.
[400] ibid art 1(35)(b). See art 47.
[401] ibid art 1(36). See art 50.

for the purposes laid down in Article 82(3).[402] Therefore, this provision adds two further derogations to the right specifically applicable to the case of Europol.

e. A new Article 39a is introduced on the maintenance of a record of all categories of processing activities under Europol's responsibility.[403]
f. The designation, position and tasks of the DPO of Europol are outlined in more detail.[404]
g. The changes in relation to supervision by the EDPS are minor, as Article 58 of Regulation (EU) 2018/1725 is not applicable to Europol. Therefore, the duties and powers of the EDPS, as laid down in Article 43(2)-(4) of the Europol Regulation, remain unchanged.
h. Coordinated supervision of Europol will take place in accordance with Article 62 of Regulation (EU) 2018/1725, therefore within the framework of the European Data Protection Board,[405] and the Cooperation Board will no longer operate.[406]

2. Article 30 concerning the processing of special categories of personal data is amended to explicitly include biometric data within special categories of personal data.[407] Furthermore, whereas until now only Europol has direct access to special categories of personal data, under the proposal Member States may also have such direct access in cases where the agency conducts dedicated operational projects and Member States may determine information be made directly accessible to selected other Member States for the purpose of enhanced collaboration.[408]

3.9.3. Need for further alignment: Enhancing the role of the EDPS and clarifying the scope of the right to restriction

The strengthening of Europol's data protection framework is of course welcome, particularly the application of Chapter IX and Article 3 of Regulation (EU) 2018/1725 to the operational data processing by the agency. With regard to the protection of biometric data as special categories of personal data, the alignment of Europol's standards to those of all other data protection legal instruments also addresses prior criticism that the Europol Regulation was unclear about the safeguards applicable to biometric data processed and the extent to which biometric personal data were losing their protective safeguards by being treated as regular personal data.[409] Therefore, these reforms must be seen as an important step towards a comprehensive alignment of the data protection framework for all EU institutions, bodies and agencies.

However, this proposal is an opportunity to address the need for **alignment of the EDPS powers in relation to Europol with the general powers of the EDPS** laid down in Article 58 of Regulation (EU) 2018/1725. Currently, the EDPS does not have the legal power to order Europol to bring processing operations into compliance with the rules of Regulation (EU) 2018/1725, to impose an administrative fine pursuant to Article 66 of that Regulation in the case of non-compliance, or to order the suspension of data flows to a recipient in a Member State, a third country or to an international organisation.[410] It is unclear why this legal fragmentation remains, although Article 98(1)(c) of Regulation (EU) 2018/1725 specifically calls on the Commission to identify any divergences that may create legal fragmentation of the data protection legislation in the EU, when conducting the review of the legal acts which regulate

[402] ibid art 1(24). See new art 37a.

[403] ibid art 1(27). See new art 39a.

[404] ibid art 1(30). See new arts 41(a) and (b).

[405] ibid art 1(33). See art 44(2).

[406] ibid art 1(34).

[407] ibid art 1(16)(a). See art 30(2).

[408] ibid art 1(16)(d). See art 30(5). Also see art 1(7) that amends art 20 to allow Member States to give such access.

[409] See Florin Coman-Kund, 'Europol's International Exchanges' (n 93); Teresa Quintel, 'Interoperable Data Exchanges Within Different Data Protection Regimes: The Case of Europol and the European Border and Coast Guard Agency' (2020) 26(1) European Public Law 205.

[410] EDPS, 'Opinion 4/2021' (n 177) para 41.

the processing of operational personal data by EU bodies, offices or agencies. Chapter IX is of general application, as evidenced by Recital 11 of Regulation (EU) 2018/1725, which requires that

> 'specific data protection rules applicable to the processing of operational personal data by EU bodies, offices or agencies when carrying out activities falling within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU should be consistent with […] the provisions of this Regulation relating to independent supervision, remedies, liability and penalties'.

With the processing of personal data so as to produce intelligence being at the heart of Europol's mission, the supervision of the EDPS with powers in full is necessary. Differentiated supervision regimes are bound to retain Europol in a privileged position, even though the capabilities of the agency have been significantly strengthened over the years and the recent proposal entails their further increase particularly through enhancing cooperation with private parties, third countries and the processing of big data.

Furthermore, the new Article 37a on the right to restriction of processing is not sufficiently clear and precise with regard to the legal possibilities to process personal data under a restriction. In addition to the two purposes laid down in Article 82(3) of Regulation (EU) 2018/1725, to which Article 37a explicitly refers, namely to ascertain the accuracy of the personal data and the use of the data as evidence, the legislative proposal introduces a new one, that is the protection of the rights of the data subject or another natural or legal person. The rationale for a differentiated regime of Europol in that respect is unclear, goes against the need for eliminating legal fragmentation and the addition of another derogation, which is arguably broadly worded, 'could in practice deprive the restriction of personal data processing of its intended effect'.[411]

3.10. Other proposed reforms

This thematic block aims to provide a concise overview of other reforms set out in the proposal outside the thematic blocks that have been discussed, in line with the Council's division of themes for discussion. Proposed reforms concerning political accountability have been left out of this analysis, as these are presented in the next Section.

In particular, the proposal revises the agency's tasks, which are either expanded or further clarified, as follows:

- Supporting Member States' special intervention units.[412]
- Cooperating with the European Union Agency for Cybersecurity (ENISA).[413]
- Supporting Member States in investigations against high risk criminals.[414]
- Supporting the Schengen evaluation and monitoring mechanism.[415]
- Supporting the EMPACT.[416]
- Supporting the Commission and the Member States in carrying out effective risk assessments by way of providing threats assessment analysis.[417]
- Clarifying how Europol may cooperate with Member States' FIUs.[418]

[411] ibid para 44.

[412] Commission, 'Europol proposal of 2020' (n 8) art 1(2)(a)(i). See art 4(1)(h).

[413] ibid art 1(2)(a)(ii). See art 4(1)(j).

[414] ibid art 1(2)(a)(iv). See new art 4(1)(q).

[415] ibid art1(2)(a)(iv). See new art 4(1)(s).

[416] ibid art 1(2)(b). See art 4(2).

[417] ibid art 1(2)(c). See art 4(3).

[418] ibid art 1(4). See art 7(8).

- Strengthening Europol's cooperation with OLAF to detect fraud, corruption and any other illegal activity affecting the financial interests of the EU.[419]
- Enabling joint operational analysis between Europol and Member States in specific investigations.[420] In that respect, the EDPS has noted that the concept of 'joint operational analyses' is mentioned in Recital 20, but is not defined in the text.[421] Furthermore, the legal rules applicable to the processing of personal data in the framework of such joint operational analyses; whereas Recital 20 mentions that the rules and safeguards will be those of the Europol Regulation, Article 20(3) foresees that the information could be accessed and further processed in accordance with national law.[422]
- Clarifying that Europol staff may provide operational support to national law enforcement authorities on the ground in operations and investigations.[423]
- Supporting Member States in informing the public about individuals wanted.[424]
- Clarifying that Member States may make the result of operational and forensic analysis provided by Europol available to their relevant authorities, including prosecutors and criminal courts.[425]
- Clarifying that Europol staff may give evidence in criminal proceedings in the Member States.[426]

3.11. Enhancing political accountability, parliamentary scrutiny and judicial control

This final part focuses on political and judicial oversight of Europol's activities and the need to ensure a better framework to provide parliamentary oversight and political scrutiny, thus enhancing Europol's democratic legitimacy.

Debates about the political accountability of Europol[427] have gone hand in hand with a progressive––yet by no means complete––relinquishment of its intergovernmental features.[428] These debates have been prompted by an increased interest of parliaments to control Europol's activities that are 'marked by efficiency, pro-activeness and pragmatism'.[429] Importantly, Article 88 TFEU explicitly provides for the involvement of the European Parliament and national parliaments in democratic oversight of Europol, as a result of an overall strengthening of their roles under the Lisbon Treaty. These debates continue to date, despite the new features of the Europol Regulation, primarily the setting up of the JPSG, as discussed in Section 2.7. In that regard, on 17 December 2020, the European Parliament adopted its Resolution on the EU Security Union Strategy for 2020-2025, calling for 'enhanced political accountability, as well as enhanced judicial control and parliamentary scrutiny, with a strong focus on accountability, transparency and respect for fundamental rights'.[430] Central in these efforts is the Common Approach on Decentralised Agencies as agreed in 2012.[431] Whereas the involvement of the

[419] ibid art 1(9). See art 21(8).

[420] ibid art 1(7)(a). See new art 20(2)(a).

[421] EDPS, 'Opinion 4/2021' (n 177) para 48.

[422] ibid.

[423] Commission, 'Europol proposal of 2020' (n 8) art 1(2)(e). See new art 4(5).

[424] ibid art 1(5); see new art 18(2)(f).

[425] ibid art 1(7)(b); See new art 20(3).

[426] ibid art 1(7)(c); See new art 20(5).

[427] Sonja Puntscher Rickmann, 'Security, Freedom and Accountability: Europol and Frontex' in Elspeth Guild and Florian Geyer (eds), *Security versus Justice? Police and Judicial Cooperation in the European Union* (Ashgate 2009).

[428] For a recent analysis on this see Kerttuli Lingenfelter and Samuli Miettinen, 'Obstacles to Supranational Operational Police Powers in the European Union: Europol Reform and the Construction of Trust between National Police Authorities' (2021) 28(2) Maastricht Journal of European and Comparative Law 182.

[429] Gless and Walh (n 79) 348.

[430] European Parliament, 'Resolution of 17 December 2020 on the EU Security Union Strategy' (P9_TA(2020)0378) para 26.

[431] For the common approach see Council, Document 11450/12 (18 June 2012).

European Parliament in the adoption and transmission of work programmes, which is a way to ensure *ex-ante* control of agencies, is in line with the Common Approach[432]—it only needs to be consulted on the multiannual work programme and should be informed of the annual programme—there is still room for improvement and parliamentary scrutiny over Europol's work remains limited. This is a first-class opportunity to re-open the debate.

Article 51 of the Europol Regulation enhanced political accountability by the European Parliament and national parliaments through the establishment of the JPSG to 'politically monitor Europol's activities in fulfilling its mission, including as regards the impacts of those activities on the fundamental rights and freedoms of natural persons'. Topics discussed in the JPSG meetings have centred on Europol's multiannual work programme, data protection, cooperation with other EU agencies, third countries, the implications of the United Kingdom's departure from the EU and right-wing terrorism.[433] Furthermore, as Schinina has noted, Europol's representatives have also repeatedly expressed their concerns for the level of resources allocated to the agency under the new Multiannual Financial Framework, in the light of its reinforced role after the adoption of the Europol Regulation.[434] Although budgetary powers are in the hands of the European Parliament, national parliaments, involved and bilaterally approached by Europol, shared Europol's concerns and promoted political initiatives to increase Europol's resources.[435] They have also made use of their right to address oral and written questions to Europol, including on Europol cooperation with the private sector and its role in operational cases related to the assassination of investigative journalists.[436]

However, whereas this reform has been welcome as having the potential to enhance the transparency, its effectiveness is questionable, not least due to structural deficiencies, given that the JPSG is supposed to meet in principle twice a year and is composed by up to four members of each national parliament and up to sixteen members of the European Parliament (that is, more than 120 persons).[437] Furthermore, the scope of parliamentary oversight itself is unclear: though the Europol Regulation does not explicitly exclude 'concrete actions taken in relation to specific operational cases',[438] as is the case of the Eurojust Regulation, the concept of 'politically monitoring' is already sufficient to exclude Europol's day-to-day work and its operational dimension.[439] As the term leaves room for interpretation, the Meijers Committee has conversely opined that scrutiny over the programming documents does not *a priori* exclude operational activities and, in particular, Europol activity in the EU external context.[440] That interpretation seems to be adopted by the Dutch Parliament, which, through questions on the multiannual programme, also addressed Europol's operational work (for instance, in the field of cooperation between Europol and the private sector).[441]

---

[432] ibid para 29.

[433] van Ballegooij (n 162) 7.

[434] See in particular the letter from the German Bundestag's delegation to the JPSG pushing national parliaments to appeal to the respective Governments and Members of the European Parliament in order to ensure a significant increase of Europol's resources in the next Multiannual Financial Framework, which may be found here <https://secure.ipex.eu/IPEXL-WEB/conference/getconference.do?type¼082dbcc5667f1c7a016681b2ccc40281> accessed 3 May 2021.

[435] Maria Schinina, 'What Balance between Eurojust and Europol from a Parliamentary Angle?' (2020) 11(2) New Journal of European Criminal Law 123, 130.

[436] van Ballegooij (n 162) 7.

[437] For an overview of such issues see Diane Fromage, 'The New Joint Parliamentary Scrutiny Group for Europol: Old Wine in New Bottles?' (*BlogActiv.eu*, 17 June 2017) <https://eutarn.blogactiv.eu/2017/06/17/the-new-joint-parliamentary-scrutiny-group-for-europol-old-wine-in-new-bottles/> accessed 3 May 2021; Chloé Brière, 'Cooperation of Europol and Eurojust with External Partners in the Fight Against Crime: What Are the Challenges Ahead?' (DCU Brexit Institute Working paper 1/2018) 22–24; Schinina (n 435) 132.

[438] Eurojust Regulation, art 67(2).

[439] Gless and Walh (n 79) 352.

[440] Meijers Committee (n 139).

[441] Schinina (n 435) 131. For an overview of the questions submitted to Europol see van Ballegooij (n 162) 9-10.

Moreover, the JPSG may request the Chair of the Management Board and the Executive Director to appear before it. However, the powers the European Parliament and the JPSG have over the Management Board from the perspective of participation are rather weak. As mentioned, Article 14(4) of the Europol Regulation foresees that the Management Board may invite any person whose opinion may be relevant for the discussion, including, where appropriate, a representative of the JPSG, to attend its meeting as a non-voting observer. The topics for which the presence of the JPSG may be relevant are Europol's programming document or budgetary aspects related to the fulfilment of Europol's activities, and, therefore, in practice a JPSG representative is invited to attend a Management Board meeting twice a year.[442] In practice, even the appointment of the JPSG Member participating in the Management Board meetings, the duration of their mandate and the modalities of reporting to the JPSG have been highly contentious,[443] thus hindering its effectiveness. Furthermore, in accordance with Article 51(5) of the Europol Regulation, the JPSG may draw up 'summary conclusions' on the political monitoring of Europol and submit those conclusions to the European Parliament and the Member States' national parliaments. The European Parliament forwards them for information purposes to the Council, the Commission and Europol. Whereas this provision is 'rather innovative in the field of cooperation among parliaments, taking into consideration that the interparliamentary meetings generally do not produce any conclusions',[444] in reality, Gless and Wahl have rightly observed that 'Europol does not have to fear direct consequences of this parliamentary scrutiny'.[445] In addition, more issues are created due to the JPSG's Rules of Procedures; for example, the rules concerning JPSG membership are not sufficient to ensure expertise and long-term continuity, as parliaments can only be encouraged to take into account competence and continuity in the appointment of their delegation. Besides, the conclusions, as all decisions of the JPSG, are decided based on consensus, which makes their adoption complicated.[446]

Further concerns about Europol's democratic accountability are connected with the position of the European Parliament: except for its budgetary powers in relation to Europol[447] and for minor rights it has been given by the Regulation, the European Parliament has a limited role in the development of internal rules concerning the functioning of Europol, the adoption of a number of which is instead delegated to the Management Board.[448]

Moreover, with regard to the **appointment of the Management Board**, the Common Approach stipulates that the European Parliament *may* designate one member on the Management Board of an agency, where appropriate (without prejudice to the relevant arrangements for existing agencies). Practice shows that the vast majority of agencies do not make use of this opportunity and the Management Boards consist exclusively of representatives of the Commission and Member States, without any involvement of the European Parliament. The sole exception, whereby involvement of the European Parliament is foreseen, is the case of the European Agency for the Cooperation of Energy Regulators (ACER), the Management Board of which includes five members appointed by the Council in addition to two members appointed by the Commission and two appointed by the European

[442] See Europol, 'Consolidated Annual Activity Report 2019'. Also see Europol, 'Consolidated Annual Activity Report 2018' 55, which reads: 'With a view to establishing a constructive and fruitful relationship with the JPSG, a key partner in ensuring and continuously strengthening Europol's democratic legitimacy and accountability to the Union's citizens, the M[anagement] B[oard] discussed throughout 2018 the practical implementation of Article 14(4) of the E[uropol] R[egulation] and, in October, agreed to invite the JPSG representative to attend two M[anagement] B[oard] meetings per year, namely one M[anagement] B[oard] meeting per semester under the auspices of the respective EU Presidency, concerning items for which the JPSG opinion was deemed relevant to the M[anagement] B[oard] discussions'.

[443] Schinina (n 435) 132.

[444] Schinina (n 435) 128.

[445] Gless and Wahl (n 79) 353.

[446] Fromage (n 437).

[447] Europol Regulation, art 58.

[448] Mitsilegas and Giuffrida (n 18).

Parliament.[449] The possible involvement of the European Parliament in the Management Board of Europol by designating a representative could be an option, but this approach has been met by the European Parliament with mixed responses; on the one hand, some consider that this would clash with the supervisory role of the European Parliament and others opine this may be a way forward for purposes of information provision and feedback, particularly in light of the large sizes of Management Boards and in cases of shared competence.[450] Given the controversial character of this potential reform, another option is to **enhance the observer role of the JPSG so that the representative could attend the Management Board on a more rigorous manner and gain more information and more awareness of what Europol is doing**.[451]

Another way in which political accountability of Europol may be increased concerns the **appointment (and removal) of the Executive Director**. According to the Common Approach on Decentralised Agencies, the appointment procedure must be simple and apolitical; the director should be appointed by the Management Board on the basis of a list of potential candidates drawn up by the Commission and resulting from a transparent selection procedure. However, research shows that there is wide variation—as evidenced by the existence of eight different models of appointment procedures—regarding the influence of the European Parliament in the appointment process, from cases where the selected candidate shall be invited to give a statement and answer questions in the European Parliament or its competent committee to lesser degrees of influence, with Europol featuring at the very end of that spectrum.[452] This is because the Executive Director is appointed by the Council from a shortlist of candidates proposed by the Management Board and the European Parliament may invite the candidate for a hearing, after which it shall give a non-binding opinion.[453] As it has been pointed out, the reason for retaining this approach is probably path dependency.[454] In the proposal for the Europol Regulation, the Commission had aligned the appointment procedure with that of other agencies, by prescribing that the Management Board would appoint the Executive Director based on a shortlist prepared by the Commission and the European Parliament could invite the candidate for a hearing.[455] However, the procedure, which in any case did not increase the European Parliament's role, was not amended. With the significant expansion of Europol's powers as demonstrated in this Study, the imperative to increase parliamentary scrutiny is the right step forward and, therefore, the revision of the Europol mandate presents a first class opportunity to further increase political accountability. This could be achieved by requiring that the selected candidate shall be invited to give a statement and answer questions in the European Parliament. As Vos has pointed out, the hearings can be regarded as 'a political tool, relying on the visibility of the hearings and the overall relationship between the agency and the E[uropean] P[arliament]'.[456]

Similarly, the Executive Director can be removed only pursuant to a decision of the Council acting on a proposal from the Management Board.[457] Thus, the European Parliament is marginalised in this procedure, as it should only be informed about the decision of the Council.[458]

---

[449] Ellen Vos, 'EU Agencies, Common Approach and Parliamentary Scrutiny' (Study for the European Parliamentary Research Service, 2018, PE 627.131) 57.

[450] Francis Jacobs, 'EU Agencies and the European Parliament' in Michelle Everson, Cosimo Monda and Ellen Vos (eds), *EU Agencies inbetween the Institutions and Member States* (Kluwer law International 2014) 221-222.

[451] Ellen Vos, 'European Agencies and the Composite EU Executive' in Michelle Everson, Cosimo Monda and Ellen Vos (eds), *European Agencies in between institutions and Member States* (Kluwer law International 2014).

[452] Vos, 'EU Agencies, Common Approach' (n 449) 59-63.

[453] Europol Regulation, art 54(2).

[454] Vos, 'EU Agencies, Common Approach' (n 449) 60-61.

[455] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA' COM(2013) 173 final, art 56.

[456] Vos, 'EU Agencies, Common Approach' (n 449) 59.

[457] Europol Regulation, art 54(7).

[458] ibid.

As regards transparency through access to information processed by Europol, there is a further limitation in relation to concerns about access to classified information. Europol mainly relies on information provided by national authorities, over which Member States have absolute control, through the 'principle of originator control'. National authorities may prevent disclosure to the European Parliament by denying their consent despite the fact that the information is available for the agency or it has an impact on fundamental rights.[459] In that respect, it has been pointed out that the 'networking platform' of the JPSG might be a way forward, as national parliaments could 'provide valuable influence in accessing information from national sources that Member States would normally be distrustful of sharing with the E[uropean] P[arliament]'.[460]

Whereas none of the aforementioned issues are addressed in the Europol proposal, there is one reform that relates to the work of the JPSG and is, therefore, worth mentioning in this Section. As mentioned in previous sections, Article 1(37) of the proposal requires additional information to be transmitted to the JPSG as per the rules in Article 51(3). That information is related to reforms on thematic blocks 1-4.

a) Annual information about the number of cases in which Europol issued follow-up requests to private parties or own-initiative requests to Member States of establishment for the transmission of personal data, including specific examples of cases demonstrating why these requests were necessary for Europol to fulfil its objectives and tasks.
b) Annual information about the number of cases where it was necessary for Europol to process personal data outside the categories of data subjects listed in Annex II in order to support Member States in a specific criminal investigation, including examples of such cases demonstrating why this data processing was necessary.
c) Annual information about the number of cases in which Europol issued alerts in the SIS and the number of 'hits' these alerts generated, including specific examples of cases demonstrating why these alerts were necessary for Europol to fulfil its objectives and tasks.
d) Annual information about the number of pilot projects in which Europol processed personal data to train, test and validate algorithms for the development of tools, including AI based tools, for law enforcement, including information on the purposes of these projects and the law enforcement needs they seek to address.

Though this is certainly a welcome feature, unless the aforementioned issues are addressed so that Europol's scrutiny is not a 'blunt sword',[461] these reforms will be of limited value.

Finally, as regards judicial control, as indicated in Section 2.6, it has been considerably strengthened compared to the pre-Lisbon days, as the CJEU may, in principle, exercise a certain level of control, not only over the validity and interpretation of the rules laid down in the Europol Regulation, but also over their actions, in accordance with the limits encompassed in the TFEU. However, the majority of the acts and decisions through which Europol accomplishes its mission still escape the CJEU's scrutiny.[462] The principles developed by the CJEU in its case law on OLAF seem applicable in this context as well. On the one hand, Europol cannot adopt coercive measures pursuant to Article 88(3) TFEU, which means that Europol's requests and acts do 'not bring about a distinct change in the [individual's] legal position', as mentioned in Article 276 TFEU and, therefore, cannot be subject to the action for annulment as per Article 263 TFEU. However, it is clear that if Europol's mandate is reformed to enable the agency to record alerts into SIS, then CJEU will clearly have jurisdiction in cases of unlawful alerts, as those cases certainly the act of Europol to record the alert would bring about a distinct change in the individual's legal position. On the other hand, national measures carried out at Europol's request cannot be reviewed by the CJEU, as Article 276 TFEU explicitly excludes the Court's jurisdiction to rule

[459] Valentin Abazi, 'The Future of Europol's Parliamentary Oversight: A Great Leap Forward' (2014) 15(6) German Law Journal: Review of Developments in German, European and International Jurisprudence 1126.

[460] Irena Ilić, 'Parliamentary Oversight of Europol under Europol Regulation 794/2016: A Modified Institutional Framework' (2019) 10 Queen Mary Law Journal, 51, 62.

[461] Gless and Wahl (n 79) 353.

[462] Mitsilegas and Giuffrida (n 18).

'on the validity or proportionality of operations carried out by the police or other law-enforcement services of a Member State'.

4. POLICY RECOMMENDATIONS

This study aimed to provide background information on the Europol Regulation and to analyse the proposal for an amendment of that Regulation. As it has been demonstrated, the reform entails considerable paradigm shifts in the way the agency operates and its relationship with the Member States and third parties. These reforms have been proposed **before an evaluation of the Europol Regulation was conducted, which hinders a proper and in-depth assessment of Europol's work. Any assessment on the impact and effectiveness of the agency can be based on minimal anecdotal information provided in the Impact Assessment, empirical work or Europol itself.**

In light of the above, the study analysed the different proposed reforms and provides the following recommendations:

(1) Enabling Europol to cooperate effectively with private parties

This reform reflects **the emergence of the growing trend to establish direct channels of communication between law enforcement and private parties and foster a public/private partnership.** Questions about the ability of private parties to undertake the role of law enforcement authorities in scrutinising fully and effectively the fundamental rights implications of transfer of personal data held by them for the purposes of law enforcement emerge, as Europol will be enabled to forward requests on behalf of Member States and proactively request information. Private parties do not enjoy equality with public authorities in terms of cooperation and the same will also apply in the case of Europol. Therefore, they may find themselves in a subordinate position, being 'cornered' by both Europol and Member States to hand over the personal data requested. Important safeguards, in particular obtaining prior judicial authorisation and scrutiny of compliance with fundamental rights, risk being bypassed. Therefore, **applying this approach to the case of Europol requires detailed rules on the duties of Europol, Member States and the private sector, as well as provisions on independent authorisation of transfers and remedies for individuals**.

The study suggests the following:

- **The nature of private parties**, which may include non-governmental organisations (NGOs), as well as financial institutions, must be clarified.
- It is welcome that in order to counter-balance the new powers of Europol the proposal maintains the existing specific safeguards, such as the requirement for 'absolute' or 'strict' necessity, as stated in Article 26(5) of the Europol Regulation.
- Furthermore, the difference between the terms 'transmission' and 'transfer,' which is observed in Article 26(5), must be explained to ensure alignment with other data protection instruments.
- **The reversed, permissive wording in Article 26(5) is questionable and it must be examined whether such change is appropriate and necessary**.
- As regards the new legal ground, further safeguards could be added in line with the pronouncements of the Impact Assessment, which states that Europol will gather information to establish the jurisdiction of the Member States concerned over a form of crime falling within the agency's mandate.
- The question as to whether the private party should be allowed to transfer the data received from Europol to any other party must be discussed.
- The **involvement of the EDPS before the agency makes such transfers, by inserting a requirement for the EDPS to be informed and by potentially involving the Europol DPO in decisions to follow up with private parties** could be explored.
- As regards revised Article 26(6) regarding transfers of personal data to private parties established in third countries, it is welcome that **the proposal proscribes systematic, massive or structural transfers**; however, the latter relates only to cases of international transfers to private parties established outside the EU, and therefore **that safeguard should apply also to transmissions to private parties within the EU**.

- With respect to the possibility of Europol proactively requesting personal data via the national units from private parties, it must be noted that **the roles of Europol and Member States are unclear**.
- **Whereas Recital 31 of the proposal refers to multi-jurisdictional and non-attributable datasets, Article 26 makes no such distinction**.
- The text could be more explicit to include safeguards mentioned in the Impact Assessment, namely that a reasoned request shall be sent which should be as targeted as possible, and should refer to the least sensitive data that is strictly necessary for Europol to establish the jurisdiction of the Member State concerned.
- The fact that national requests would have to be subject to prior judicial authorisation and provide access to an effective remedy could also be mentioned in the text, as stressed in the Impact Assessment.
- **It must be specified that Member States and private parties are not obliged to cooperate in this respect.**
- It should be clarified whether following a request Europol could receive the data directly from the private party (thus the information would belong to Europol, and the latter would not have to inform the Member State(s) concerned) or through the Member State only (thus qualifying the information as national information).
- In addition, as regards the role and responsibilities of Europol when acting as service provider to national authorities by offering its infrastructure for exchanges of data between Member States and private parties, these are also not sufficiently clear. The only guidance offered is in the Impact Assessment, whereby in a footnote it is stated that '[i] these cases Europol acts as data processor rather than as data controller'. The Europol Regulation does not define the concept of 'data processor'.
- As regards Europol's role in supporting Member States to prevent the dissemination of online content related to terrorism and violent extremism, this should be aligned with the prescriptions of the recently adopted Regulation 2021/784 on that matter. The authorisation of the Executive Director requires further criteria in line with those mentioned in Article 26(6). Finally, the term 'crisis situation' must be defined.

(2) Enabling Europol to process large and complex datasets

In response to the EDPS' admonishment of Europol, the proposal introduces the concept of 'pre-analysis' of large and complex datasets received solely to separate necessary information, within the scope of Article 18(5) and Annex II, from data unrelated to criminal activity. As this reform will have substantial impact on the protection of personal data, enhanced safeguards must be introduced so that it is ensured that **this exception does not become the rule**.

- It is welcome that the prior processing is limited to a maximum period of one year, which can be extended following authorisation by the EDPS. Deletion of unnecessary data is also foreseen.
- Definitions of the term 'large datasets' and potentially that of 'digital forensics' could be added.
- Pre-analysis must be further limited to cases where the transfer by Member States to Europol and the subsequent processing of large datasets is actually an objective necessity.
- The way in which the extension of the maximum period of pre-analysis will work in practice, given the lack of any indication and criteria to determine the existence of a 'justified case,' must be clarified.
- The involvement of the EDPS prior to each pre-analysis must be enhanced and the DPO could be required to provide authorisation.
- The relationship between the new derogation under Article 18(5a) and the existing derogation under Article 18(6) of the Europol Regulation, which enables processing of data for the purpose of determining whether such data are relevant to its task, requires clarification. The retention periods should also be aligned if necessary.

- The relationship between Article 18(5a) and 18(a) also requires clarification.
- The term 'investigative case file' is crucial to determine the scope of applicability of Article 18a and, therefore, as this rule is an exception, the term must not be defined expansively.
- An expansion of the scope of Article 18a beyond operational analyses goes against the exceptional character of the derogation
- The criteria that would be applied to determine that it is an exceptional and duly justified case are perhaps in that respect unclear, and the intervention of the EDPS could be foreseen. As for the assessment provided by Europol that will have been recorded, it could be sent to the EDPS for their information.
- It must be prescribed that rules on the scale of the processing, as well as on the complexity, type or importance of investigations must be introduced by the Management Board of Europol.
- The involvement of the EDPS in cases where an investigative case file has been submitted by a third country should be maintained.
- It should be further required that if there are preliminary indications that such data is disproportionate or collected in violation of fundamental rights, Europol shall not only refrain from processing the data but also *delete* that data.
- The last sentence of Article 18a(4) that data will be shared within the EU is also vital, and, as far as is possible, it must be ensured that products of Europol's analysis are not further disseminated by third countries to their own partners.

(3) Strengthening Europol's role on research and innovation

With Europol acquiring a pioneering role in shaping the future of law enforcement tools, this study found that some safeguards are included in the proposal, but there is room for improvement, as follows:

- The term 'innovation activities' must be defined so as to ensure consistency in the terminology used across legal instruments in data protection law;
- As developing new technologies extensive processing of large quantities of personal data may be required, processing of operational personal data must be accompanied by efficient and appropriate safeguards:
  (a) the processing of personal data for research and innovation should take place only if needed in order to reach the objectives of the project;
  (b) the possibility of using synthetic, anonymised or pseudo-anonymised personal data where possible, should be foreseen;
  (c) the processing of special categories of personal data, which are sensitive in nature should be explicitly excluded or accompanied by appropriate safeguards on the purpose for processing, the actors that would have access to that sensitive data and the accountability framework;
  (d) the principles of data minimisation, data quality and privacy by design and by default;
  (e) the scope of the research and innovation activities should be further refined by specifically and concretely linking the activities with the tasks of Europol and clarifying their scope in a binding document, for instance adopted by the Management Board of Europol, which could be subsequently updated, if necessary. That binding document should be available to the EDPS prior to the launch of each project for information and consultation and the EDPS could be updated every time the document is updated, as appropriate; and
  (f) the one-year retention period of the logs may not be sufficient for data protection purposes and, therefore, logs could also be kept for an additional period, so as to enable the EDPS to conduct supervision and audits.
- The synergies with Member States and other agencies involved in research and innovation should be clarified.
- The potential involvement of Europol in the screening of specific cases of different investments into the EU concerning undertakings that provide technologies used or

developed by Europol or by Member States for the prevention and investigation of crimes does not fall within Europol's mandate and should be discarded.

(4) Enabling Europol to enter data into the Schengen Information System (SIS)

This reform is particularly controversial, thus diverging approaches have emerged with certain Member States having substantial reservations as to the possibility for Europol to enter alerts into SIS, and others broadly supporting the Commission proposals possibly with some amendments.

Overall, the possibility of enabling Europol to record alerts in SIS presents **numerous legal and operational challenges as regards the nature of SIS and the agency, quality of information, fundamental rights of individuals and possible conflict with national law and investigations**. It marks another important shift in both the identity of SIS as an information system and in the operational powers of Europol. In that respect, it is unclear as to **whether Europol's mandate supports this shift, which essentially places Europol, whose work is covered with some secrecy and non-transparency, on an equal footing with Member States.** It will also undermine the reliability of SIS, the opacity of which in the processes of entering alerts has been subject to criticism.

The study has raised questions as to whether—and how—Europol will handle the issuance of alerts and analyse information received from third countries or organisations so as to undertake a meaningful quality check. As a result, if this reform progresses, the study recommends:

- To clarify the criteria that will be employed to qualify specific third countries as trusted as we all as the criteria that will be used to verify the reliability and accuracy of information.
- To prescribe specific indications as to when Europol will halt the procedure and decide not to enter an alert.
- To consider co-opting Member States in a (joint) verification process through consultation. To some extent, this will enable Member States to use their own resources to verify the reliability of the alert, and decide whether they would be willing or able to enter an alert on their own in case of a specific national interest. This approach would be in line with the existing informal Protocol developed by the Terrorism Working Party and endorsed by the Standing Committee on Operational Cooperation on Internal Security (COSI) in November 2020.
- To enquire on the use of the informal Protocol so as to determine whether that tool is sufficient.
- To clarify the operational value of 'information alerts,' as the proposal is vague on the action to be taken at the national level, and this discretion may lead to misuses of the alerts by third countries, abuses at the national level during border controls, and divergent practices with significant impact on the individuals concerned.
- To consider the option of improving the availability of Interpol alerts so that these can be better used, and in that respect to enquire as to why there is limited information on the countries where Interpol alerts are not visible to all front-line officers.

If the compromise solution of enabling Europol to enter alerts related to counter-terrorism is adopted, the aforementioned concerns remain the same; this reform will merely **serve as the gateway to further expand Europol's powers to enter alerts into SIS in the future.**

In any case, the qualification of a third country as 'trusted' may raise significant concerns and, therefore, the existence of an agreement between Europol and a third country is by no means sufficient.

(5) Strengthening Europol's cooperation with third countries

This study found that the change in the text to enable the Executive Director to authorise 'categories of transfers of personal data' is unclear. It must be viewed in conjunction with Article 38 of the Law Enforcement Directive, which prescribes a similar rule. In that respect the study proposes:

- The term 'categories of transfers' must be clarified, strictly circumscribed and differentiated from the terms 'sets of transfers' as mentioned in Article 25(6) and 'group of transfers,' so as to avoid being used for surveillance activities in general, thus changing Europol's powers.
- More information on the implementation and practical application of Article 38 of the Law Enforcement Directive must be provided.

The addition of a new provision adding new grounds for transferring personal data to third countries on the basis of appropriate safeguards must not be accepted, as it is highly problematic due to serious institutional and fundamental rights concerns.

From an institutional perspective, it is an effort to bypass the legal ground for the transfer of personal data provided by an international agreement on the basis of Article 218 TFEU, and hence of the European Parliament's right to give consent. As a result, it constitutes a major step backwards in terms of political accountability.

From a fundamental rights perspective, it constitutes a major disregard to the constitutional limits provided by the CJEU in *Schrems* as regards the importance that the data protection framework in the third country must be adequate, understood as equivalent to that of the EU. It is unclear how in practice this could work when the legally binding document is an agreement between a Member State and a third country.

(6) Strengthening Europol's cooperation with the European Public Prosecutor's Office (EPPO)

The proposed rules must be **aligned to those of the EPPO Regulation and the working arrangement between the two agencies**. Therefore, it must be clarified that:

- Europol may support the investigation of the EPPO *following a request by the latter*.
- Article 20a must expressly set out the rules that pertain to Europol's cooperation with the EPPO, or that at least Article 20a refers to the specific paragraphs of Article 21 that are applicable *mutandis mutandis*.
- In reference to 'active support,' the activities of the EPPO take their cue from Recital 69 of the EPPO Regulation, but that wording is not found in the body of that Regulation.
- As for the possibility of Europol to support the EPPO in investigations *and* prosecutions, the working arrangement concluded between the two agencies prescribes that Europol provides assistance to EPPO in criminal investigations only and, therefore, the reference to prosecutors must be deleted.

(7) Enabling Europol to request the initiation of an investigation of a crime affecting a common interest covered by an EU policy

This proposed reform is disproportionate in light of the supportive role of Europol, as it removes control from judicial authorities over the opening of their investigations in cases affecting one Member State only, and the concept of 'crime which affects a common interest covered by an EU policy' is particularly vague and may be interpreted in a particularly expansive manner. It is recommended that the wording of this rule remain unchanged.

(8) Strengthening the data protection framework applicable to Europol

The strengthening of Europol's data protection framework, by applying Article 3 and Chapter IX of Regulation (EU) 2018/1725 to Europol and by envisaging biometric data as special categories of personal data, is of course welcome. Therefore, these reforms must be seen as an important step towards a comprehensive alignment of the data protection framework for all EU institutions, bodies and agencies.

This proposal is an opportunity to address the need for **alignment of the EDPS powers in relation to Europol with the general powers of the EDPS** laid down in Article 58 of Regulation (EU) 2018/1725. This is all the more necessary as the proposal entails a considerable increase in Europol's mandate,

particularly through enhancing cooperation with private parties, third countries and the processing of big data.

Furthermore, the new Article 37a on the right to restriction of processing should be aligned with Article 82(3) of Regulation (EU) 2018/1725, as the need for a differentiated regime is not substantiated.

(9) Enhancing political accountability and parliamentary scrutiny

The Europol Regulation enhanced political accountability and parliamentary scrutiny, primarily through the setting up of the JPSG; the Commission's proposal requires that additional information be provided to the JPSG.

Its effectiveness is questionable, not least due to structural deficiencies and the lack of clarity as to the scope of the scrutiny and the weak powers of the JPSG. In light of the above, this study recommends:

- To clarify that the scope of the scrutiny conducted by the JPSG includes operational activities.
- To consider the potential streamlining of the membership and participation to the JPSG, e.g. on the basis of expertise and long-term continuity.
- To strengthen the powers of the JPSG in the Management Board in terms of participation, e.g. by envisaging the need for the Management Board to follow up on the summary conclusions of the JPSG and by enabling the representative to attend the Management Board on a more rigorous manner and gain more information and more awareness of what Europol is doing.

In order to further enhance the role of the European Parliament, possible ways forward are the following:

- To explore the possibility that a member of the Management Board being designated by the European Parliament.
- To increase the European Parliament's influence in the appointment and removal of the Executive Director, e.g. by prescribing that the Management Board would appoint the Executive Director based on a shortlist prepared by the Commission and the European Parliament must invite the candidate for a hearing.

As a final remark, it must be emphasised that any additional powers to Europol and the EDPS must be accompanied by the **appropriate funding and staff to fulfill their tasks**.

REFERENCES

- Abazi, V., 'The Future of Europol's Parliamentary Oversight: A Great Leap Forward' (2014) 15(6) *German Law Journal* 1126.
- Anderson, M. and others*, Policing the European Union,* Clarendon Press, Oxford, 1995.
- Azoulai, L. and Van Der Sluis, M., 'Institutionalizing Personal Data Protection in Times of Global Institutional Distrust: Schrems' (2016) 53(5) *Common Market Law Review* 1343.
- Bigo, D. and others, *The Field of the EU Internal Security Agencies*, L'Harmatan/Centre d'études sur les conflits, Paris, 2007.
- Brière, C., 'Cooperation of Europol and Eurojust with External Partners in the Fight Against Crime: What Are the Challenges Ahead?' (DCU Brexit Institute Working paper 1/2018).
- Brouwer, E., 'Schengen's Undesirable Aliens' in Paul Minderhoud, Sandra Mantu and Karin Zwaan (eds), *Caught in between Borders - Citizens, Migrants, Humans: Liber Amicorum in honour of prof.dr. Elspeth Guild* (Wolf Legal Publishers, Nijmegen, 2019).
- _____, *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System*, Martinus Nijhoff, Leiden, 2008.
- Busuioc, M., *European Agencies. Law and Practices of Accountability*, Oxford University Press, Oxford, 2013.
- Busuioc, M. and Curtin, D., 'The EU Internal Security Strategy, the EU Policy Cycle and the Role of (AFSJ) Agencies. Promise, Perils and Pre-requisites' (Study for the European Parliament LIBE Committee, PE 453.185 2011).
- Carrera, S., Stefan, M. and Mitsilegas, V., 'Cross-Border Data Access in Criminal Proceedings and the Future of Digital Justice' (CEPS, October 2020).
- Cocq, C. and Galli, F., 'The Evolving Role of Europol in the Fight Against Serious Crime: Current Challenges and Future Prospects' in Saskia Hufnagel and Carole McCartney (eds), *Trust in International Police and Justice Cooperation* (Hart, London, 2017).
- Coman-Kund, F., *European Union Agencies as Global Actors: A Legal Study of the European Aviation Safety Agency, Frontex and Europol*, Routledge, Oxfordshire, 2018.
- _____, 'Europol's International Exchanges of Data and Interoperability of AFSJ Databases' (2020) 26(1) *European Public Law* 181.
- _____, 'Europol's International Cooperation between 'Past Present' and 'Present Future': Reshaping the External Dimension of EU Police Cooperation' (2018) 2(1) *Europe and the World* 1.
- Commission, 'A Europe that Protects: EU Crisis Protocol: responding to terrorist content online' (October 2019)

  https://ec.europa.eu/home-affairs/sites/default/files/what-we-do/policies/european-agenda-security/20191007_agenda-security-factsheet-eu-crisis-protocol_en.pdf.
- Cooper, I., 'A New Form of Democratic Oversight in the EU: The Joint Parliamentary Scrutiny Group for Europol' (2018) 10(3) *Perspectives on Federalism* 185.
- Coudert, F., 'The Europol Regulation and Purpose Limitation: From the 'Silo-Based Approach' to … What Exactly?' (2017) 3(3) *European Data Protection Law Review* 313.

- Council, 'Declaration of the Home Affairs Ministers of the European Union - Ten points on the future of Europol' (21 October 2020).
- Council, Document 5527/6/21 (23 April 2021).
- _____, Document 5388/4/21 (23 April 2021).
- _____, Document 7732/21 (13 April 2021).
- _____, Document 5388/3/21 (9 April 2021).
- _____, Internal Document WK 3974/2021 (19 March 2021).
- _____, Document 14308/1/20 (18 March 2021).
- _____, Document 5527/4/21 (5 March 2021).
- _____, Document 5388/2/21 (5 March 2021).
- _____, Document 5397/21 (19 January 2021).
- _____, Document 13083/1/20 (24 November 2020).
- _____, Document 13037/30 (16 November 2020).
- _____, Document 13037/20 (11 November 2020).
- _____, Document 11512/20 (9 October 2020).
- _____, Document 8868/20 (16 June 2020).
- _____, Document 14745/19 (2 December 2019).
- _____, Document 12837/19 (7-8 October 2019).
- _____, Document 10494/20 (4 July 2019).
- _____, Document 9680/18 (4 June 2018).
- _____, Document 11450/12 (18 June 2012).
- _____, Document 5970/02 (8 February 2002).
- _____, 'The Development of Europol's missions: Non Paper submitted by France and Greece on the creation of alerts in the SIS', as mentioned in Council, Document 7732/21 (13 April 2021).
- De Buck, B., 'Joint Investigation Teams: The Participation of Europol Officials' (2007) 8(2) *ERA Forum* 253.
- De Moor, A. and Vermeulen, G., 'The Europol Council Decision: Transforming Europol into an Agency of the European Union' (2010) 47(4) *Common Market Law Review* 1089.
- Disley, E. and others, 'Evaluation of the implementation of the Europol Council Decision and of Europol's activities', Technical Report for Europol Management Board, Rand Europe, 2012.
- Drewer, D. and Miladinova, V., 'The BIG DATA Challenge: Impact and Opportunity of Large Quantities of Information Under the Europol Regulation' (2017) 33(3) *Computer Law & Security Review* 298.
- European Data Protection Supervisor (EDPS), 'Opinion 4/2021 – EDPS Opinion on the Proposal for Amendment of the Europol regulation' (8 March 2021).

- _____, 'EDPS Decision of 17 September 2020 relating to EDPS own initiative inquiry on Europol's big data challenge' (18 September 2020).
- _____, 'Opinion 3/2020 on the European Strategy of Data' (16 June 2020).
- _____, 'EDPS Formal comments on the draft Commission Implementing Regulation laying down rules and conditions for the operation of the web service and data protection and security rules applicable to the web service pursuant to Article 13 of Regulation (EU) 2017/2226 and repealing Commission Implementing Decision C(2019)1230' (13 February 2019).
- _____, 'EDPS Decision on the own initiative inquiry on Europol's big data challenge (5 October 2020).
- 'EU: More powers for Europol: what does your government think?' (*Statewatch*, 15 March 2021) https://www.statewatch.org/news/2021/march/eu-more-powers-for-europol-what-does-your-government-think/.
- 'EU: Warnings over proposed new Europol partners in Middle East and North Africa' (*Statewatch*, 14 May 2018)

  <https://www.statewatch.org/news/2018/may/eu-warnings-over-proposed-new-europol-partners-in-middle-east-and-north-africa/.
- European Union Agency for Fundamental Rights (FRA), 'Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Regulation on preventing the dissemination of terrorist content online' (12 February 2019).
- Europol, 'Europol's main operational considerations in light of the Europol Regulation' (14 July 2020) https://www.statewatch.org/media/1284/eu-europol-operational-considerations-legal-basis-edoc-1119771v3.pdf.
- _____, 'Written contribution to JPSG The Europol Innovation Lab - May 2020' (28 May 2020) https://www.europarl.europa.eu/cmsdata/208046/Europol%20Contribution%20for%20Electronic%20exchange%20-%20Europol%20Innovation%20Lab.pdf.
- _____, 'Europol Strategy 2020+' (2019) https://www.europol.europa.eu/publications-documents/europol-strategy-2020.
- _____, 'Consolidated Annual Activity Report 2019'.
- _____, 'Consolidated Annual Activity Report 2018'.
- _____, 'Europol Strategy 2016-2020' (2016) https://www.europol.europa.eu/publications-documents/europol-strategy-2016-2020.
- Fletcher, M., Lööf, R. and Gilmore, B., *EU Criminal Law and Justice*, Edward Elgar Publishing, Cheltenham, UK, Northampton, MA, USA, 2008.
- Fromage, D., 'The New Joint Parliamentary Scrutiny Group for Europol: Old Wine in New Bottles?' (*BlogActiv.eu*, 17 June 2017) https://eutarn.blogactiv.eu/2017/06/17/the-new-joint-parliamentary-scrutiny-group-for-europol-old-wine-in-new-bottles/.
- Gless, S., 'Europol' in Valsamis Mitsilegas, Maria Bergström and Theodore Konstadinides (eds), *Research Handbook on EU Criminal Law* (Edward Elgar Publishing, Cheltenham, UK, Northampton, MA, USA, 2016).

- Gless, S. and Pfirter, P., 'Cross-Border Access and Exchange of Digital Evidence: Cloud Computing Challenges to Human Rights and the Rule of Law' in Valsamis Mitsilegas and Niovi Vavoula (eds), *Surveillance and Privacy in the Digital Age: European, Transatlantic and Global Perspectives* (Hart, London, 2021).
- Gless, S. and Wahl, T., 'A Comparison of the Evolution and Pace of Police and Judicial Cooperation in Criminal Matters: A Race Between Europol and Eurojust?' in Chloé Brière and Anne Weyembergh (eds), *The Needed Balances in EU Criminal Law: Past, Present and Future* (Hart, London, 2018).
- Groenleer, M., *The Autonomy of the European Union Agencies: A Comparative Study of Institutional Development*, Uitgeverij Eburon, Delft, 2009.
- Gruszczak, A., 'The EU Criminal Intelligence Model' in Joanna Beata Banach-Gutierrez and Christopher Harding (eds), *EU Criminal Law and Policy - Values, Principles and Methods* (Routledge, Oxfordshire, 2017).
- Guild, E. and others, 'Implementation of the EU Charter of Fundamental Rights and its Impact on EU Home Affairs Agencies - Frontex, Europol and the European Asylum Support Office' (Study for the European Parliament LIBE Committee, PE 453.196 2011).
- Hayes, B. and others, 'The Law Enforcement Challenges of Cybercrime: Are We Really Playing Catch-Up?' (Study for the European Parliament LIBE Committee, PE 536.471 2015).
- Heimans, D., 'The External Relations of Europol – Political, Legal and Operational Considerations' in Berndt Martenczuk and Servaas van Thiel (eds), *Justice, Liberty and Security: New Challenges for EU External Relations* (VUBPRESS, Brussels, 2008).
- Hinnant, L., 'France puts 78,000 security threats in vast police database' (*Associated Press*, 4 April 2018) https://apnews.com/a1690ac25cea4d5b8d2b622d3fd4e646/France-puts-78,000-security-threats-on-vast-police-database.
- Hufnagel, S., *Policing Global Regions: The Legal Context of Transnational Law Enforcement Cooperation*, Routledge, Oxfordshire, 2021.
- _____, 'Organized Crime' in Valsamis Mitsilegas, Maria Bergström and Theodore Konstadinides (eds), *Research Handbook on EU Criminal Law* (Edward Elgar Publishing, Cheltenham, UK, Northampton, MA, USA, 2016).
- Ilić, I., 'Parliamentary Oversight of Europol under Europol Regulation 794/2016: A Modified Institutional Framework' (2019) 10 *Queen Mary Law Journal* 51.
- Jacobs, F., 'EU Agencies and the European Parliament', in Michelle Everson, Cosimo Monda and Ellen Vos (eds), *EU Agencies in between the Institutions and Member States* (Kluwer law International, Alphen aan den Rijn, 2014).
- Klip, A., *European Criminal Law: An Integrative Approach,* 3rd edn, Intersentia, Cambridge, 2016.
- Ligeti, K. and Robinson, G., 'Sword, Shield and Cloud: Toward a European System of Public-Private Orders for Electronic Evidence in Criminal Matters?' in Valsamis Mitsilegas and Niovi Vavoula (eds), *Surveillance and Privacy in the Digital Age: European, Transatlantic and Global Perspectives* (Hart, London, 2021).
- Lingenfelter, K. and Miettinen, S., 'Obstacles to Supranational Operational Police Powers in the European Union: Europol Reform and the Construction of Trust between National Police Authorities' (2021) 28(2) *Maastricht Journal of European and Comparative Law* 182.

- Meijers Committee, 'Note on the interparliamentary scrutiny of Europol' (CM 1702).
- Milieu, 'Study on the practice of direct exchanges of personal data between Europol and private parties' (September 2020).
- Mitsilegas, V. and Giuffrida, F., 'Bodies, Offices and Agencies' in Valsamis Mitsilegas, *EU Criminal Law* (2nd edn, Hart, London, forthcoming 2021).
- Mitsilegas, V., 'Extraterritorial Immigration Control, Preventive Justice and the Rule of Law in Turbulent Times: Lessons from the Anti-Smuggling Crusade' in Juan Santos Vara, Sergio Carrera and Tineke Strik (eds), *Constitutionalising the External Dimension of EU Migration Policies in Times of Crisis: Legality, Rule of Law and Fundamental Rights Reconsidered* (Edward Elgar Publishing, Cheltenham, UK, Northampton, MA, USA, 2019).
- _____, 'The Privatisation of Mutual Trust in Europe's Area of Criminal Justice: The Case of E-evidence' (2018) 25(3) *Maastricht Journal of European and Comparative Law* 263.
- Occhipinti, J.D., *The Politics of EU Police Cooperation - Toward a European FBI?*, Lynne Rienner, Boulder and London, 2003.
- Puntscher Rickmann, S., 'Security, Freedom and Accountability: Europol and Frontex' in Elspeth Guild and Florian Geyer (eds), *Security versus Justice? Police and Judicial Cooperation in the European Union* (Ashgate, Farnham, 2009).
- Quintel, T., 'Interoperable Data Exchanges Within Different Data Protection Regimes: The Case of Europol and the European Border and Coast Guard Agency' (2020) 26(1) *European Public Law* 205.
- Rijken, C., 'Joint Investigation Teams: Principles, Practice, and Problems. Lessons Learnt from the First Efforts to Establish a JIT' (2006) 2(2) *Utrecht Law Review* 99.
- Scherrer, A., Jeandesboz, J. and Guittet, E.P., 'Developing an EU Internal Security Strategy, Fighting Terrorism and Organised Crime' (Study for the European Parliament LIBE Committee, PE 462.423 2011).
- Schinina, M., 'What Balance between Eurojust and Europol from a Parliamentary Angle? (2020) 11(2) *New Journal of European Criminal Law* 123.
- Sheptycki, J., Jaffel, H.B. and Bigo, D., 'International Organised Crime in the European Union' (Study for the European Parliament LIBE Committee, PE 462.420 2011).
- Van Ballegooij, W., 'Revision of the Europol Regulation' (January 2021).
- Van Duyne, P.C. and Vander Beken, T., 'The Incantations of EU Organised Crime Policy' (2009) 51(2) *Crime, Law and Social Change* 261.
- Vavoula, N., *Immigration and Privacy in the Law of the European Union; The Case of Information Systems*, Brill Nijhoff, Leiden, forthcoming 2021.
- _____, 'The European Commission package of ETIAS consequential amendments: Substitute impact assessment' (Study for the Directorate-General for Parliamentary Research Services (EPRS) of European Parliament, PE 642.808 2019).
- Vos, E., 'EU Agencies, Common Approach and Parliamentary Scrutiny' (Study for the European Parliamentary Research Service, PE 627.131 2018).

- _____,'European Agencies and the Composite EU Executive' in Michelle Everson, Cosimo Monda and Ellen Vos (eds), *European Agencies in between Institutions and Member States* (Kluwer law International, Alphen aan den Rijn, 2014).
- Wahl, T., ' The European Union as an Actor in the Fight Against Terrorism ' in Marianne Wade and Almir Maljevic (eds), *A War on Terror?* (Springer, Cham, 2010).

Case law:

- Case C362/14 *Maximillian Schrems v Data Protection Commissioner* ECLI:EU:C:2015:650.
- Opinion 1/15 ECLI:EU:C:2017:592.
- *Weber and Saravia v Germany* (2008) 46 EHRR SE5.

This study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee, aims to provide background information on the current legal framework of Europol and a legal assessment of the European Commission's proposal of 9 December 2020 to strengthen Europol's mandate, divided in thematic blocks. The legal assessment is accompanied by policy recommendations.

PE 694.200
IP/C/LIBE /2021-018

Print ISBN 978-92-846-8094-8| doi: 10.2861/53707| QA-05-21-140-EN-C
PDF ISBN 978-92-846-8095-5| doi: 10.2861/799884| QA-05-21-140-EN-N